Anexa nr. 22
la Documentația standard nr.115

din “15” septembrie 2021

Specificaţii tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Procedura de achiziție: Program Antivirus pentru protecția infrastructurii informaționale						
MTender ID: ocds-b3wdp1-MD-1717052514298 din 30.05.2024						
Denumirea bunurilor/serviciilor	**Denumirea modelului bunului/serviciului**	**Ţara de origine**	**Producătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standard de referinţă**
1	2	3	4	5	6	7
Bunuri/servicii						
Program Antivirus pentru protecția infrastructurii informaționale	Bitdefender GravityZone Business Security Premium	România	Bitdefender	Specificații pentru soluție de protecție si securitate antivirus pentru protectia infrastructurii: Se solicita achizitia a unei soluții corporative de tip anti-malware, care sa ofere protecțiea, securitatea si scanarea vulnerabilităților a 500 de stații de	Specificații pentru soluție de protecție si securitate antivirus pentru protectia infrastructurii ofertată: Soluți corporativă de tip anti-malware **Bitdefender GravityZone Business Security Premium**, care oferă protecție, securitate si scanarea	

				lucru, servere fizice si virtualizate, cutii postale pentru o perioadă de 12 luni. Produsul (solutia) sa reprezinte o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul trebuie sa contina urmatoarele module: 1. O consola de management care asigura functionalitati de administrare. 2. Protectie statii si servere fizice/virtuale. 3. Protectie si securitate pentru serverele email Microsoft Exchange Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST, AV-Comparatives, etc.) 1. Instalare si configurare: 1. Masinile de scanare (pentru tipul de scanare centralizata) pentru mediile virtuale se descarca din interfata web a produsului. 2. Cerinte generale:	vulnerabilităților a 500 de stații de lucru, servere fizice si virtualizate, cutii postale pentru o perioadă de 12 luni. Produsul ofertat reprezintă o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul contine urmatoarele module: 1. O consola de management care asigura functionalitati de administrare. 2. Protectie statii si servere fizice/virtuale. 3. Protectie si securitate pentru serverele email Microsoft Exchange Produsul antivirus oferit ocupă locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST, AV-Comparatives, etc.) 1. Instalare si configurare: 1. Masinile de scanare (pentru tipul de scanare centralizata) pentru mediile virtuale se descarca din interfata web a produsului. 2. Cerinte generale:	

				1. Interfata consolei de management trebuie sa fie inclusiv in limba romana. 2. Interfata clientului de securitate, care se instaleaza pe statii si servere, trebuie sa fie inclusiv in limba romana. 3. Manualul de instalare a produsului trebuie sa fie inclusiv in limba romana. 4. Manualul de administrare a produsului trebuie sa fie inclusiv in limba romana. 5. Solutia trebuie sa pemita activarea/dezactivarea actualizarilor de produs/semnaturi. 6. Actualizari automate a consolei de management facute de catre producatorl solutiei, fara interventia utilizatorului. 7. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trebuie trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile). 8. Consola de management trebuie sa fie accesibila de oriunde in lume (solutie de tip Cloud), fara a	1. Interfata consolei de management este inclusiv in limba romana. 2. Interfata clientului de securitate, care se instaleaza pe statii si servere, este inclusiv in limba romana. 3. Manualele de instalare a produsului sunt prezentate in limba romana, limba rusă si engleză. 4. Manualele de administrare a produsului sunt prezentate in limba romana, limba rusă si engleză. 5. Solutia pemite activarea/dezactivarea actualizarilor de produs/semnaturi. 6. Actualizari automate a consolei de management facute de catre producatorl solutiei, fara interventia utilizatorului. 7. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, pot fi trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile). 8. Consola de management este accesibila de oriunde in lume (solutie de tip Cloud), fara a	

				fi nevoie de setari suplimentare din partea utilizatorului. 9. Consola de management trebuie sa fie accesibila atat de pe statii de lucru cat si de pe dispozitive mobile (smartphone, tableta). **3. Panou de monitorizare si raportare (Dashboard):** 1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata). 2. Panoul central trebuie sa contina rapoarte pentru toate modulele suportate. 3. Rapoartele din panoul central de comanda trebuie sa permita: adaugarea altor rapoarte, stergerea lor si rearanjarea. 4. Inventarierea retelei – managementul securitatii: 1. Solutia trebuie sa se integreze cu domeniul Active Directory si sa poata importa inventarul. 2. Solutia trebuie sa se permita descoperirea statiilor statii fizice neintegrate in Active	fi nevoie de setari suplimentare din partea utilizatorului. 9. Consola de management este accesibila atat de pe statii de lucru cat si de pe dispozitive mobile (smartphone, tableta). **3. Panou de monitorizare si raportare (Dashboard):** 1. Rapoartele din panoul de monitorizare 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 permite: adaugarea altor rapoarte, stergerea lor si rearanjarea. 4. Inventarierea retelei – managementul securitatii: 1. Solutia se integreză cu domeniul Active Directory si sa poata importa inventarul. 2. Solutia permite descoperirea statiilor statii fizice neintegrate in Active Directory	

				Directory (Workgroup) cu ajutorul Network discovery. 3. Solutia trebuie sa ofere 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 trebuie sa se permita 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 trebuie sa se permita instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale. 6. Solutia trebuie sa se permita selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 7. Solutia trebuie sa se permita lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.	(Workgroup) cu ajutorul Network discovery. 3. Solutia oferă 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 trebuie sa ofere posibilitatea de repornire a masinilor fizice de la distanta. 9. Solutia trebuie sa ofere informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes. 10. Solutia trebuie sa se permita configurarea centralizata a clientilor antimalware prin intermediul politicilor 11. Solutia trebuie sa ofere in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi. 5. Politici: 1. Solutia trebuie sa se permita configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module 2. Politica trebuie sa contina 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.	8. Solutia oferă posibilitatea de repornire a masinilor fizice de la distanta. 9. Solutia oferă 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 oferă in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi. 5. Politici: 1. Solutia permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module 2. Politica contine 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 trebuie sa permita aplicarea politicilor pe masini client, grupuri de masini, domeniu, unitati organizationale. 4. Politica sa poate fi schimbata automat in functie de: a. IP sau clasa de IP al statiei b. Gateway-ul alocat c. DNS serverul alocat d. WINS serverul alocat e. Sufix DNS pentru conexiunea dhcp f. Clientul este/nu este in acceasi retea cu infrastructura de management (statia de lucru poate solutiona implicit numele gazdei) g. Tipul retelei (lan, wireless) 6. Rapoarte: 1. Solutia trebuie sa contina rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate. 2. Rapoartele programate sa poata fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management). 3. Solutia trebuie sa permita vizualizarea rapoartelor curente programate de administrator.	3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, domeniu, unitati organizationale. 4. Politica poate fi schimbata automat in functie de: a. IP sau clasa de IP al statiei b. Gateway-ul alocat c. DNS serverul alocat d. WINS serverul alocat e. Sufix DNS pentru conexiunea dhcp f. Clientul este/nu este in acceasi retea cu infrastructura de management (statia de lucru poate solutiona implicit numele gazdei) g. Tipul retelei (lan, wireless) 6. Rapoarte: 1. Solutia contine rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate. 2. Rapoartele programate pot 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 trebuie sa permita exportarea rapoartelor in format .pdf si detaliile ca format .csv. 5. Solutia trebuie sa includa 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 trebuie sa includa 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	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) 8. Interogarea legata de evenimente Exchange include informatii precum: a. Directia traficului e-mail b. Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atasate) c. Masurile implementate in fiecare situatie (curatarea, stergerea, inlocuirea sau carantinarea fisierului, stergerea sau respingerea e-mail-ului) 7. Carantina: 1. Solutia trebuie sa permita restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila. 2. Carantina trebuie sa fie locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de management.	c. starea modulelor si rolurilor de protectie instalate pe agentul de securitate d. denunmirea si alocarea politicii e. utilizatorul autentificat in timpul evenimentului f. evenimente (site-uri blocate, aplicatii blocate, detectiile etc) 8. Interogarea legata de evenimente Exchange include informatii precum: a. Directia traficului e-mail b. Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atasate) c. Masurile implementate in fiecare situatie (curatarea, stergerea, inlocuirea sau carantinarea fisierului, stergerea sau respingerea e-mail-ului) 7. Carantina: 1. Solutia permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila. 2. Carantina este locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de management.	

				8. Utilizatori: 1. Administrarea trebuie sa se poata 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. Solutia trebuie sa permita configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari. 5. Solutia trebuie sa permita 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 se poate 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. Solutia permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari. 5. Solutia 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. Solutia trebuie sa ofere informatii detaliate pentru fiecare actiune a unui utilizator. 3. Solutia trebuie sa permita filtrarea actiunilor utilizator dupa numele utilizatorului, actiune. 10. Actualizare: 1. Solutia trebuie sa permita definirea de locatii de actualizare multiple. 2. Solutia trebuie sa permita activarea/dezactivarea actualizarilor de produs si semnaturi. 3. Orice client antivirus trebuie sa poata fi configurat sa livreze update-urile catre alt client antivirus 4. Solutia trebuie sa permita 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:	9. Log-uri: 1. Inregistrarea actiunilor utilizatorilor. 2. Solutia oferă informatii detaliate pentru fiecare actiune a unui utilizator. 3. Solutia permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune. 10. Actualizare: 1. Solutia permite definirea de locatii de actualizare multiple. 2. Solutia permite activarea/dezactivarea actualizarilor de produs si semnaturi. 3. Orice client antivirus poate fi configurat sa livreze update-urile catre alt client antivirus 4. Solutia permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizari de produs:	

				a. Ciclu rapid, gandit pentru un mediu de test in cadrul retelei b. Ciclu lent, gandit pentru restul retelei (productie, servere critice etc) 5. Solutia trebuie sa permita stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management. B. PROTECTIE STATII SI SERVERE FIZICE/VIRTUALE 1. Caracteristici generale minimale si eliminatorii: 1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall). 2. Pentru o mai buna protectie a statiilor si serverelor, solutia trebuie sa includa un vaccin anti-ransomware. Acest vaccin trebuie sa asiasigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor,	a. Ciclu rapid, gandit pentru un mediu de test in cadrul retelei b. Ciclu lent, gandit pentru restul retelei (productie, servere critice etc) 5. Solutia permite stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management. B. PROTECTIE STATII SI SERVERE FIZICE/VIRTUALE 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 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 asiasigură 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 trebuie sa primeasca actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware. 4. Pentru o mai buna protectie a statiilor si serverelor, solutia trebuie sa includa protectie impotriva atacurilor zero-day de tip exploit avansate (atacuri directionate) bazata pe tehnologii de invatare automata (machine learning). 5. Pentru o mai buna protectie a a statiilor si serverelor, solutia trebuie sa includa un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un numar mare de riscuri existente la nivel de retea sau sistem de operare ce pot afecta functionalitatea si nivelul de securizare al endpoint-ului 6. Pentru o mai buna protectie a statiilor si serverelor, solutia trebuie sa includa un modul avansat de securitate - HyperDetect, bazat pe tehnologii de tip „machine learning tunabil”,proiectat special pentru a	chiar daca sunt infectate si prin blocarea procesului de criptare. 3. Vaccinul anti-ransomware primește actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware. 4. Pentru o mai buna protectie a statiilor si serverelor, solutia include protectie impotriva atacurilor zero-day de tip exploit avansate (atacuri directionate) bazata pe tehnologii de invatare automata (machine learning). 5. Pentru o mai buna protectie a a statiilor si serverelor, solutia include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un numar mare de riscuri existente la nivel de retea sau sistem de operare ce pot afecta functionalitatea si nivelul de securizare al endpoint-ului 6. Pentru o mai buna protectie a statiilor si serverelor, solutia include un modul avansat de securitate - HyperDetect, bazat pe tehnologii de tip „machine learning tunabil”,proiectat special pentru	

				detecta atacuri avansate si activitati suspecte in faza pre-executie. 7. Acest modul avansat de securitate va proteja impotriva: atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de retea suspect, exploit-urilor, ransomware si grayware. Fiecarui tip de amenintare mentionat, i se vor putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv. 8. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, sterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide daca doreste intai monitorizare sau doreste si blocarea amenintarilor. Aceste actiuni mentionate, vor putea fi stabilite independent, pentru fisiere sau pentru traficul din retea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenintarile care ar fi fost detectate daca nivelul de protectie era stabilit mai agresiv). 9. Pentru a oferi un nivel aditional de protectie a statiilor si serverelor, solutia trebuie sa	a detecta atacuri avansate si activitati suspecte in faza pre-executie. 7. Acest modul avansat de securitate va proteja impotriva: atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de retea suspect, exploit-urilor, ransomware si grayware. Fiecarui tip de amenintare mentionat, i se vor putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv. 8. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, sterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide daca doreste intai monitorizare sau doreste si blocarea amenintarilor. Aceste actiuni mentionate, vor putea fi stabilite independent, pentru fisiere sau pentru traficul din retea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenintarile care ar fi fost detectate daca nivelul de protectie era stabilit mai agresiv). 9. Pentru a oferi un nivel aditional de protectie a statiilor si	

				includa un sandbox in cloud-ul public al producatorului acesteia. 10. Modulul de Sandbox va putea trimite automat fisiere in Sandbox-ul din cloud-ul producatorului unde vor putea fi „detonate” pentru o analiza in profunzime. 11. Modulul de Sandbox trebuie sa includa doua variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul va putea accesa fisierul dorit, pe cand in modul blocare, utilizatorului i se va bloca rularea fisierului pana cand Sandbox-ul din cloud-ul producatorului va da verdictul. 12. Modulul de Sandbox trebuie sa includa doua tipuri de actiuni remediere: implicita si de siguranta. Pentru actiunea implicita se va putea stabili: doar raportare, dezinfectie, stergere si carantinare. Pentru actiunea de siguranta se va putea stabili: stergere sau carantinare. 13. Modulul de Sandbox trebuie sa includa 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	serverelor, solutia include un sandbox in cloud-ul public al producatorului acesteia. 10. Modulul de Sandbox va putea trimite automat fisiere in Sandbox-ul din cloud-ul producatorului unde vor putea fi „detonate” pentru o analiza in profunzime. 11. Modulul de Sandbox include doua variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul va putea accesa fisierul dorit, pe cand in modul blocare, utilizatorului i se va bloca rularea fisierului pana cand Sandbox-ul din cloud-ul producatorului va da verdictul. 12. Modulul de Sandbox include doua tipuri de actiuni remediere: implicita si de siguranta. Pentru actiunea implicita se va putea stabili: doar raportare, dezinfectie, stergere si carantinare. Pentru actiunea de siguranta se va putea stabili: stergere sau carantinare. 13. Modulul de Sandbox include si posibilitatea de trimitere manuala a fisierelor in Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malitios, il poate	

				trimite manual in Sandbox pentru a fi „detonat” si a afla verdictul. Va putea trimite mai multe fisiere de odata, cu posibilitate de a specifica daca vor fi „detonate” individual sau toate in acelasi timp. 14. Modulul de Sandbox trebuie sa suporte „detonarea” urmatoarelor tipuri de fisiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. 15. Fisierele mentionate anterior, vor putea fi detectate corect chiar daca sunt incluse in arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. 2. Cerinte de sistem: • Sisteme de operare pentru statii de lucru:	trimite manual in Sandbox pentru a fi „detonat” si a afla verdictul. Va putea trimite mai multe fisiere de odata, cu posibilitate de a specifica daca vor fi „detonate” individual sau toate in acelasi timp. 14. Modulul de Sandbox suportă „detonarea” urmatoarelor tipuri de fisiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. 15. Fisierele mentionate anterior, pot fi detectate corect chiar daca sunt incluse in arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. 2. Cerinte de sistem: • Sisteme de operare pentru statii de lucru:	

				• Windows 10 November 2022 Update (22H2) • Windows 11 September 2022 Update (22h2) • Windows 11 (initial release) • Windows 10 November 2021 Update (21H2) • Windows 10 May 2021 Update (21H1) • Windows 10 October 2020 Update (20H2) • Windows 10 May 2020 Update (20H1) • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone 5) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 Creators Update (Redstone 2) • Windows 10 Anniversary Update (Redstone 1) • Windows 10 November Update (Threshold 2) • Windows 10 (initial release) • Windows 8.1 • Windows 8 • Windows 7 • macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X	• Windows 10 November 2022 Update (22H2) • Windows 11 September 2022 Update (22h2) • Windows 11 (initial release) • Windows 10 November 2021 Update (21H2) • Windows 10 May 2021 Update (21H1) • Windows 10 October 2020 Update (20H2) • Windows 10 May 2020 Update (20H1) • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone 5) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 Creators Update (Redstone 2) • Windows 10 Anniversary Update (Redstone 1) • Windows 10 November Update (Threshold 2) • Windows 10 (initial release) • Windows 8.1 • Windows 8 • Windows 7 • macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X	

				Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12), • Sisteme de operare embedded: Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7 • Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016 , Windows Server 2016 (Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, , Windows Server 2008 R2, • Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 36-38 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Amazon Linux 2023, Google COS Milestones 77,81,85,	Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12), • Sisteme de operare embedded: Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7 • Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016 , Windows Server 2016 (Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, , Windows Server 2008 R2, • Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 36-38 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Amazon Linux	

				Azure Mariner 2, AlmaLinux 8,9.x, Rocky Linux 8.x, Cloud Linux 7,8.x, Pardus 21, Linux Mint 20.x,21.x , Miracle 8.x.,Oracle Linux 7.x-9.x UEK-RHCK, Rocky Linux 8-9.x, Cloud Linux 7-8.x, Kylinv10 RHEL, Debian 9-12, PopOS 22.04, Pardus 21, SLES 12-15 SP1-SP5, 3. Administrare si instalare remote: 1. Inainte de instalare, administratorul trebuie sa poata repartiza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 2. Instalarea se va putea face in mai multe moduri: a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea; b. prin instalarea la distanta, direct din consola de management c. trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac. 3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus	2023, 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.x,21.x , Miracle 8.x.,Oracle Linux 7.x-9.x UEK-RHCK, Rocky Linux 8-9.x, Cloud Linux 7-8.x, Kylinv10 RHEL, Debian 9-12, PopOS 22.04, Pardus 21, SLES 12-15 SP1-SP5, 3. Administrare si instalare remote: 1. Inainte de instalare, administratorul poate repartiza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 2. Instalarea se poate face in mai multe moduri: a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea; b. prin instalarea la distanta, direct din consola de management c. trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac. 3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client	

				existent in locatiile respective pentru a minimiza traficul in WAN. 4. In consola trebuie sa fie disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc. 5. Din consola trebuie sa se poata trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere. 6. Consola trebuie sa includa 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 trebuie sa poata crea grupuri sau chiar	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, politica aplicata, informatii despre actualizari etc. 5. Din consola se poate trimite 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 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 avea posibilitatea de a crea grupuri	

				subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu. 11. Solutia trebuie sa permita 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 trebuie sa permita administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul trebuie sa poata alege intre urmatoarele actiuni: a. Actiune imiplicita pentru fisiere infectate: - interzice accesul - dezinfecteaza - stergere - muta fisierele in carantina - nicio actiune b. Actiune alternativa pentru fisierele infectate: - interzice accesul - dezinfecteaza - stergere - muta fisierele in carantina	sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu. 11. Solutia permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu. 4. Caracteristici si functionalitati principale ale modulului antimalware: 1. Solutia permite administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul va putea alege intre urmatoarele actiuni: a. Actiune imiplicita pentru fisiere infectate: - interzice accesul - dezinfecteaza - stergere - muta fisierele in carantina - nicio actiune b. Actiune alternativa pentru fisierele infectate: - interzice accesul - dezinfecteaza - stergere - muta fisierele in carantina	

				c. Actiune imiplicita pentru fisierele suspecte: - interzice accesul - 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, trebuie sa	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 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, poate anula	

				poata 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 trebuie sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese. 9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware. 10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa 11. Produsul antimalware trebuie sa poata 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.	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 permite 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 oferă protectie anti-spyware. 10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa 11. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea.	

				12. Administratorul trebuie sa poata 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	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 comportamentul fisierelor si bazata pe monitorizarea proceselor. 14. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP. 15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul trebuie sa includa optiunea de setare a unei parole pentru protectia la dezinstalare. 16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing. 17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata. 5. Anti-Exploit-Avansat: 1. Solutia trebuie sa ofere 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.	Scanare hibrid (cloud public cu motoare light) 13. Pentru o protectie sporita, solutia antimalware pune la dispoziție 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor. 14. Pentru o protectie sporita, solutia antimalware poate scana paginile HTTP. 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 oferă protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata. 5. Anti-Exploit-Avansat: 1. Solutia oferă 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	

				3. Protejarea aplicatiilor utilizate frecvent si a celor de tip „sistem” cum ar fi browserele, aplicatiile de tip office sau reader, procesele critice aferente sistemelor de operare. 6. Firewall: 1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate. 2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 3. Posibilitatea de a defini retele de incredere pentru masina destinatie. 4. Abilitatea de a detecta scanarea de porturi. 5. Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune 7. Carantina: 1. Produsul antimalware trebuie sa permita trimiterea automata a fisierelor din carantina	vulnerabiliza un sistem de operare. 3. Protejarea aplicatiilor utilizate frecvent si a celor de tip „sistem” cum ar fi browserele, aplicatiile de tip office sau reader, procesele critice aferente sistemelor de operare. 6. Firewall: 1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate. 2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 3. Posibilitatea de a defini retele de incredere pentru masina destinatie. 4. Abilitatea de a detecta scanarea de porturi. 5. Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune 7. Carantina: 1. Produsul antimalware permite trimiterea automata a fisierelor din carantina catre	

				catre laboratoarele antimalware ale producatorului. 2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator. 3. Produsul antimalware trebuie 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 trebuie sa permita rescanarea obiectelor dupa fiecare actualizare de semnaturi. 8. Protectia datelor: 1. Produsul trebuie sa permita blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. 9. Controlul continutului: 1. Consola trebuie sa aiba integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati: a. Solutia trebuie sa permita blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.	laboratoarele antimalware ale producatorului. 2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator. 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 de a restaura un fisier din carantina in locatia lui originala. 5. Modulul de carantina permite rescanarea obiectelor dupa fiecare actualizare de semnaturi. 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 are integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati: a. Solutia permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.	

				b. Solutia trebuie sa permita blocarea accesului la Internet pe intervale orare. c. Solutia trebuie sa permita blocarea paginilor de internet care contin anumite cuvinte cheie. d. Solutia trebuie sa permita controlul accesului numai la anumite pagini de internet specificate de administrator; e. Solutia trebuie sa permita blocarea accesului la anumite aplicatii definite de administrator; f. Solutia trebuie sa permita restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). 10. Controlul dispozitivelor: 1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 2. Modulul trebuie sa permita 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	b. Solutia permite blocarea accesului la Internet pe intervale orare. c. Solutia permite blocarea paginilor de internet care contin anumite cuvinte cheie. d. Solutia permite controlul accesului numai la anumite pagini de internet specificate de administrator; e. Solutia permite blocarea accesului la anumite aplicatii definite de administrator; f. Solutia permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). 10. Controlul dispozitivelor: 1. Modulul poate fi instalat/dezinstalat in 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 trebuie sa permita configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client. 4. Modulul trebuie sa permita configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. 11. Power User: 1. Modulul trebuie sa poate fi instalat/dezinstalat in functie de preferinta administratorului. 2. Modulul trebuie sa permita 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.	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 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. 11. Power User: 1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client. 3. Modificarile efectuate din modulul Power User vor fi active local, pe masina pe care s-au facut respectivele modificari.	

				4. Administratorul trebuie sa poata suprascrie din consola setarile aplicate de utilizatorii Power User. 12. 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. C. PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE Cerinte minime de sistem: • Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox • Exchange server 2010 cu rold de Edge Transport, Hub Transport sau Mailbox 1. Produsul trebuie sa ofere protectie antimalware, antispam (inclusiv antiphishing), precum si filtrare de atasamente si continut,	4. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User. 12. 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. C. PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE Cerinte minime de sistem: • Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox • Exchange server 2010 cu rold de Edge Transport, Hub Transport sau Mailbox 1. Produsul oferă protectie antimalware, antispam (inclusiv antiphishing), precum si filtrare de atasamente si continut, prin	

				prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange. 2. Produsul trebuie sa asigure scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail. 3. Actualizarea antimalware trebuie sa poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere. 4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware va trebui sa includa si scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca. 5. Produsul trebuei sa ofere optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina). 6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul	integrarea cu serverul Microsoft Exchange. De asemenea, permite scanarea antimalware la cerere a bazelor de date Exchange. 2. Produsul asigură scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail. 3. Actualizarea antimalware poate fi facuta automat la un interval de maxim 1 ora, precum si la cerere. 4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware include si scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca. 5. Produsul oferă optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina). 6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe,	

				va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale. 7. Produsul trebuie sa ofere protectie antispam, cu o baza de semnaturi actualizabila prin internet. 8. Modulul antispam va trebui sa includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice. 9. Produsul va trebui sa ofere filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje. 10. Produsul va trebui sa ofere un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute. 11. Produsul va oferi posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori.	produsul va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale. 7. Produsul oferă protectie antispam, cu o baza de semnaturi actualizabila prin internet. 8. Modulul antispam include un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice. 9. Produsul oferă un filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje. 10. Produsul oferă un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute. 11. Produsul oferă posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori. 12. Actualizarea produsului va fi configurabila si se va putea	

				12. Actualizarea produsului va fi configurabila si se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu. 13. Produsul va trebui sa ofere statistici atat referitoare la scanarea antivirus cat si la scanarea antispam. 14. Produsul se va integra in cadrul consolei de management unitar al solutiei antivirus. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web. 4. ALTE CERINȚE OBLIGATORII: - Pentru soluția ofertată se solicită suport local și de la producător pentru 12 luni. - Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local. - Lucrările de instalare, configurare, punerea în funcţiune a soluției trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comerciala. - Se va oferi manual de instalare si administrare a produsului ofertat in limba romana si engleza.	realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu. 13. Produsul oferă statistici atat referitoare la scanarea antivirus cat si la scanarea antispam. 14. Produsul se va integra in cadrul consolei de management unitar al solutiei antivirus. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web. 4. ALTE CERINȚE OBLIGATORII: - Pentru soluția ofertată se va oferi atât suport local și de la producător pentru 12 luni. - Producătorul va oferi suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local. - In ofertă sunt incluse lucrările de instalare, configurare, punerea în funcţiune a soluției. - Se oferă manual de instalare si administrare a produsului ofertat in limba romana si engleza.	

				- Prezentarea a minim 2 certificate tehnice a persoanelor certificate pe produsul ofertat. - Ofertantul va prezenta Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat. - Ofertantul va pune la dispoziție cel puțin o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informațiilor conform ISO/IEC 27001:2018 in cazul apariție problemelor de securitate; - Termen de livrare: 10 zile lucrătoare de la data semnării contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.	- Vă prezentăm 2 certificate tehnice a persoanelor certificate pe produsul ofertat. - Prezentăm Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat. - Punem la dispoziție o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informațiilor conform ISO/IEC 27001:2018 in cazul apariție problemelor de securitate; - Termen de livrare: 10 zile lucrătoare de la data semnării contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.	

Numele, Prenumele: Cristea Ala
În calitate de: Administrator
Ofertantul: DECA SOFTWARE S.R.L.
Adresa: str. Independenței, 40, MD-2072, mun Chisinau, Republica Moldova
Semnat:_____

Digitally signed by Cristea Ala
Date: 2024.06.01 21:08:12 EEST
Reason: MoldSign Signature
Location: Moldova