XONTECH

Anexa nr.22
La Documentația
standard
aprobată prin ordinul MF nr. 115
din "15" septembrie 2021

Specificații 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,]

Numărul procedurii de achiziție: **ocds-b3wdp1-MD-1768474589356** din **15.01.2026**

Obiectul de achiziției: **Subscripția soluției corporative antivirus (EDR/EPP)**

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Cod CPV – 48761000-0 Subscripția anuală și licențe suplimentare prin upgrade a soluției corporative antivirus existente în cadrul AAC pentru o perioadă de 36 luni Licente pentru stații de lucru fizice/virtualizat - 100; Licente pentru servere fizice/virtualizate - 5.	**1.** WithSecure Elements EDR and EPP for Computers Premium license for 3 years – 100 licențe **2.** WithSecure Elements EDR and EPP for Servers Premium License for 3 years – 5 licențe	**Finlanda**	**WithSecure**	Conform Caiet de sarcini	Conform Anexei la formular. Matricea de conformitate	

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizica: Str. Ștefan cel Mare și Sfânt 73/1
NBC – National Business Center, of. 101
MD-2012, Chisinau, R.M.

B.C. MOLDOVA-AGROINDBANK S.A.,
Chișinău, Moldova.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

Semnat:
Nume: Irina Vicol
În calitate de: Administrator
Ofertantul: SC Xontech Systems SRL
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.

Digitally signed by Vicol Irina
Date: 2026.01.21 15:27:51 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizica: Str. Ștefan cel Mare și Sfânt 73/1
NBC – National Business Center, of. 101
MD-2012, Chisinau, R.M.

B.C. MOLDOVA-AGROINDBANK S.A.,
Chișinău, Moldova.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

XONTECH

Anexa

Matricea de conformitate conform Conform Caiet de sarcini – Termeni de referinta solicitate in SIA RSAP

Nr. d/o	Denumirea bunurilor solicitate	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant
1.	Subscripția anuală și licențe suplimentare prin upgrade a soluției corporative antivirus existente în cadrul AAC pentru o perioadă de 36 luni Licente pentru stații de lucru fizice/virtualizat - 100; Licente pentru servere fizice/virtualizate - 5.	Soluție integrată pentru managementul securității endpoint-urilor, gândita ca o soluție modulara și scalabilă, bazata pe tehnologia Cloud, pentru a minimiza resursele locale. **Se solicită achiziționarea subscripției anuale și licențe suplimentare prin upgrade a soluției corporative antivirus existente in cadrul AAC pentru o perioadă de 36 luni (Data expirării licențelor existente 15/01/2026):** **1. Licențe existente: 90 stații de lucru fizice/virtualizat:** WithSecure Elements EPP for Computers Premium **Licențe solicitate in cadrul procedurii: 100 stații de lucru fizice/virtualizat:** WithSecure Elements EDR and EPP for Computers Premium **2. Licențe existente: 4 servere fizice/virtualizate:** WithSecure Elements EPP for Servers Premium **Licențe solicitate in cadrul procedurii: 5 servere fizice/virtualizate:** WithSecure Elements EDR and EPP for Servers Premium **Cerințe minime de calificare a ofertanților:** - Producătorul trebuie să ofere suport tehnic 24/7, inclusiv în limba română prin e-mail sau telefon; - Suport tehnic local 24/7 în limba romana din partea partenerului local; - Autorizarea de la Producător a partenerului vis-a-vis de dreptul de vânzare și de a oferi suport tehnic produselor ofertate pe teritoriul R. Moldova;	Se oferă o Soluție integrată pentru managementul securității endpoint-urilor, gândita ca o soluție modulara și scalabilă, bazata pe tehnologia Cloud, pentru a minimiza resursele locale. **Se oferă subscripția anuala și licențe suplimentare prin upgrade a soluției corporative antivirus existente in cadrul AAC pentru o perioadă de 36 luni:** **1. Licențe solicitate in cadrul procedurii: 100 stații de lucru fizice/virtualizat:** WithSecure Elements EDR and EPP for Computers Premium **2. Licențe solicitate in cadrul procedurii: 5 servere fizice/virtualizate:** WithSecure Elements EDR and EPP for Servers Premium **Cerințe minime de calificare a ofertanților:** - Producătorul oferă suport tehnic 24/7, inclusiv în limba română prin e-mail sau telefon; - Suport tehnic local 24/7 în limba romana din partea Xontech Systems SRL; - Autorizarea de la Producător a partenerului vis-a-vis de dreptul de vânzare și de a oferi suport tehnic produselor ofertate pe teritoriul R. Moldova este anexat;

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizica: Str. Ștefan cel Mare și Sfânt 73/1
NBC – National Business Center, of. 101
MD-2012, Chisinau, R.M.

B.C. MOLDOVA-AGROINDBANK S.A.,
Chișinău, Moldova.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

		- Prezentarea documentelor confirmative a minim 2 specialiști certificați pe soluția propusa. - Ofertantul va prezenta copia Certificatului ISO 27001:2013, in domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT si de securitate, inclusiv teste de penetrare - certificat confirmat cu aplicarea semnăturii electronice. - Ofertantul va prezenta Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware si software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea si managementul infrastructurii IT si de Securitate – certificat confirmat cu aplicarea semnăturii electronice; - Ofertantul va fi certificat cu un certificat de management ISO 20000-1:2018 în domeniul furnizării de servicii de management al serviciilor IT, inclusiv implementare și suport tehnic în perioadele de pre-garanție, garanție și post-garanție, pentru sistemele informatice. - Ofertantul va avea minim o persoană certificată în calitate de lead auditor intern pentru sistemul de management al securității informaționale conform ISO/IEC 27001:2022; - Referințe de implementare in Republica Moldova in cadrul instituțiilor de stat – minim 3 referințe. **Termenii și condițiiIe de livrare/prestare/executare solicitat:** 10 zile lucrătoare de la data întrării in vigoare finuntrcafriuiin ien vai gsooalurefie ai. contrcatului, care inlcude și timpul lucrărilor de instalare, configurare și punerea în funcțiune. **<u>În cazul în care se va oferi o soluție alternativă decît cea existentă,</u> acesta trebuie să întrunească minim cerințele de mai jos, care este echivalentul soluției instalate deja în cadrul instituției:** **CONSOLA DE MANAGEMENT**	- Certificările confirmative a 2 specialiști certificați pe soluția propusa anexate cu oferta. - Anexat cu oferta este copia Certificatului ISO 27001:2023, in domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT si de securitate, inclusiv teste de penetrare - certificat confirmat cu aplicarea semnăturii electronice. - Anexat cu oferta este copia Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware si software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea si managementul infrastructurii IT si de Securitate – certificat confirmat cu aplicarea semnăturii electronice; - Anexat cu oferta este copia certificat de management ISO 20000-1:2018 în domeniul furnizării de servicii de management al serviciilor IT, inclusiv implementare și suport tehnic în perioadele de pre-garanție, garanție și post-garanție, pentru sistemele informatice. - Anexat cu oferta este copia unei persoani certificată în calitate de lead auditor intern pentru sistemul de management al securității informaționale conform ISO/IEC 27001:2022; - Referințe de implementare in Republica Moldova in cadrul instituțiilor de stat – minim 3 referințe. **Termenii și condițiiIe de livrare/prestare/executare solicitat:** 10 zile lucrătoare de la data întrării in vigoare a contractului, care inlcude și timpul lucrărilor de instalare, configurare și punerea în funcțiune. Solutia ofertata este cea existenta in infrastructura AAC si prin upgrade-ul solicitat va corespunde tuturor cerintelor specificate in caietul de sarcini. **CONSOLA DE MANAGEMENT**

		1. Cerințe generale: 1.1. Consola de management și baza de date vor fi incluse fără a fi nevoie de softuri și licențe adiționale. 1.2. Interfața consolei de management va fi în limba română sau engleză. 1.3. Interfața clientului de securitate, care se instalează pe stații și servere, va fi în limba română sau engleză. 1.4. Soluția va include un modul de update server prin care se asigura actualizarea de produs și a semnăturilor. 1.5. Notificări - Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru următoarele acțiuni: blocat, redenumit, oprit, șters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat și acțiune suplimentară solicitată de la utilizator, mutat în coșul de gunoi și ulterior expediata către o cutie poștală sau mai multe. 1.6. Soluția va permite integrarea cu un server Syslog ori SIEM pentru raportarea evenimentelor. 1.7. Soluția permite crearea unei copii de siguranța a profilului de configurație. **Panou de monitorizare și raportare (Dashboard):** 2.1. Rapoartele vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport. 2.2. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. **Inventarierea rețelei - managementul securității:** 3.1. Se permite descoperirea mașinilor din Microsoft Hyper-V. 3.2. Se permite descoperirea stațiilor fără protecție în Active Directory. 3.3. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.	**1. Functionalitati generale:** 1.1. Soluția ofertată deține o consola unică de management și baza de date incluse fără a fi nevoie de softuri și licențe adiționale. 1.2. Interfața consolei de management este în limba engleză. 1.3. Interfața clientului de securitate, care se instalează pe stații și servere, este în limba română, engleză, rusa și altele. 1.4. Soluția include un modul de update server prin care se asigura actualizarea de produs și a semnăturilor. 1.5. Notificări - Soluția permite setarea și configurarea de alerte, declanșarea poate fi aplicată pentru următoarele acțiuni: blocat, redenumit, oprit, șters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat și acțiune suplimentară solicitată de la utilizator, mutat în coșul de gunoi și ulterior expediata către o cutie poștală sau mai multe. 1.6. Soluția permite integrarea cu un server Syslog ori SIEM pentru raportarea evenimentelor. 1.7. Soluția permite crearea unei copii de siguranța a profilului de configurație. **Panou de monitorizare și raportare (Dashboard):** 2.1. Rapoartele pot fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport. 2.2. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. **Inventarierea rețelei - managementul securității:** 3.1. Se permite descoperirea mașinilor din Microsoft Hyper-V. 3.2. Se permite descoperirea stațiilor fără protecție în Active Directory. 3.3. Soluția oferă opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.

		3.4. Soluția va permite instalarea la distanță sau manual a clienților anti-malware pe mașini fizice/virtuale. 3.5. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 3.6. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare de la distanță pentru endpoint-uri. 3.7. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanță. 3.8. Soluția va oferi informații detaliate despre fiecare task și va afișa dacă task-ul s-a finalizat cu succes sau nu. 3.9. Soluția va permite configurarea centralizată a clienților anti-malware prin intermediul politicilor. 3.10. Se vor oferi în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizări, Versiunea produsului, Versiunea de semnături. 3.11. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. **4. Politici:** 4.1. Soluția va permite configurarea setărilor clientului anti-malware prin intermediul politicilor ce conțin setări pentru toate modulele. 4.2. Politica va conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea anti-malware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user. **5. Rapoarte:** 5.1. Soluția va conține rapoarte care prezintă starea endpoint-urilor din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.	3.4. Soluția permite instalarea la distanță sau manual a clienților anti-malware pe mașini fizice/virtuale. 3.5. Soluția permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 3.6. Soluția permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare de la distanță pentru endpoint-uri. 3.7. Soluția oferă posibilitatea de repornire a mașinilor fizice de la distanță. 3.8. Soluția oferă informații detaliate despre fiecare task și va afișa dacă task-ul s-a finalizat cu succes sau nu. 3.9. Soluția permite configurarea centralizată a clienților anti-malware prin intermediul politicilor. 3.10. Se oferă în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizări, Versiunea produsului, Versiunea de semnături. 3.11. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. **4. Politici:** 4.1. Soluția permite configurarea setărilor clientului anti-malware prin intermediul politicilor ce conțin setări pentru toate modulele. 4.2. Politica conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea anti-malware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user. **5. Rapoarte:** 5.1. Soluția conține rapoarte care prezintă starea endpoint-urilor din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.

		5.2. Soluția va permite vizualizarea rapoartelor curente programate de administrator. 5.3. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. 5.4. Interogarea legata de starea terminalului include informații precum: 5.4.1. tip endpoint; 5.4.2. infrastructura rețelei căreia ii aparține endpointul; 5.4.3. datele agentului de securitate; 5.4.4. starea modulelor de protecție; 5.5. Interogarea legata de evenimente endpoint include informații precum: 5.5.1. endpoint-ul pe care a avut loc evenimentul; 5.5.2. tipul starea și configurația agentului de securitate instalat; 5.5.3. starea modulelor și rolurilor de protecție instalate pe agentul de securitate; 5.5.4. denumirea și alocarea politicii; 5.5.5. utilizatorul autentificat în timpul evenimentului; 5.5.6. evenimente (site-uri blocate, aplicații blocate, detecțiile etc); **6. Carantină:** 6.1. Soluția va permite restaurarea fișierelor din carantină în locația originala. 6.2. Carantină va fi locala, pe fiecare stație administrată și va fi administrată, fie local, fie din consola de management. **7. Utilizatori:** 7.1. Administrarea se va putea face pe baza de roluri predefinite (Administrator, Auditor) sau roluri personalizate. 7.2. Administrator companie: administrează arhitectura consolei de management și serviciile de securitate;	5.2. Soluția permite vizualizarea rapoartelor curente programate de administrator. 5.3. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. 5.4. Interogarea legata de starea terminalului include informații precum: 5.4.1. tip endpoint; 5.4.2. infrastructura rețelei căreia ii aparține endpointul; 5.4.3. datele agentului de securitate; 5.4.4. starea modulelor de protecție; 5.5. Interogarea legata de evenimente endpoint include informații precum: 5.5.1. endpoint-ul pe care a avut loc evenimentul; 5.5.2. tipul starea și configurația agentului de securitate instalat; 5.5.3. starea modulelor și rolurilor de protecție instalate pe agentul de securitate; 5.5.4. denumirea și alocarea politicii; 5.5.5. utilizatorul autentificat în timpul evenimentului; 5.5.6. evenimente (site-uri blocate, aplicații blocate, detecțiile etc); **6. Carantină:** 6.1. Soluția permite restaurarea fișierelor din carantină în locația originala. 6.2. Carantină va fi locala, pe fiecare stație administrată și va fi administrată, fie local, fie din consola de management. **7. Utilizatori:** 7.1. Administrarea este pe baza de roluri predefinite (Administrator, Auditor) sau roluri personalizate. 7.2. Administrator companie: administrează arhitectura consolei de management și serviciile de securitate;

		7.3. Auditor: monitorizează și generează rapoarte. 7.4. Utilizatorii pot fi creați în consola de management. 7.5. Se va permite configurarea detaliata a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. **8. Log-uri:** 8.1. înregistrarea acțiunilor utilizatorilor. 8.2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator. 8.3. Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. **9. Actualizare:** 9.1. Se permite definirea de locații de actualizare multiple. 9.2. Se permite activarea/dezactivarea actualizărilor de produs și semnături. 9.3. Se permite actualizarea produsului într-o rețea fără acces la Internet. 9.4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus 9.5. Soluția dispune de un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat din Cloud, fără intervenția administratorului. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, poate descarcă pachetele pentru modul de scanare centralizata în mediile de virtualizare Hyper-V. 9.6. In cadrul serverului de actualizare, pentru o mai buna urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric:	7.3. Auditor: monitorizează și generează rapoarte. 7.4. Utilizatorii pot fi creați în consola de management. 7.5. Se permite configurarea detaliata a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. **8. Log-uri:** 8.1. înregistrarea acțiunilor utilizatorilor. 8.2. Se oferă informații detaliate pentru fiecare acțiune a unui utilizator. 8.3. Se permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. **9. Actualizare:** 9.1. Se permite definirea de locații de actualizare multiple. 9.2. Se permite activarea/dezactivarea actualizărilor de produs și semnături. 9.3. Se permite actualizarea produsului într-o rețea fără acces la Internet. 9.4. Orice client antivirus poate fi configurat să livreze update-urile către alt client antivirus 9.5. Soluția dispune de un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat din Cloud, fără intervenția administratorului. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, poate descarcă pachetele pentru modul de scanare centralizata în mediile de virtualizare Hyper-V. 9.6. In cadrul serverului de actualizare, pentru o mai buna urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, se va vizualiza un jurnal de modificări în care sunt precizate istoric:

		9.6.1. versiunea pachetului; 9.6.2. data versiunii; 9.6.3. funcții noi și îmbunătățiri; 9.6.4. probleme rezolvate; 9.6.5. probleme cunoscute. 9.7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului anti-malware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizări de produs: 9.8. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei 9.9. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 9.10. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. 9.11. Soluția oferă posibilitatea de actualizare a aplicațiilor învechite instalate pe stațiile de lucru. **10. Certificate:** 10.1. Accesul la consola de management să se facă doar prin HTTPS. 10.2. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitenta, data eliberării și data expirării certificatelor eliberate. **11. Caracteristici generale:** 11.1. Pentru reducerea la minim a consumului de resurse, soluția anti-malware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției anti- malware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 11.2. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția	9.6.1. versiunea pachetului; 9.6.2. data versiunii; 9.6.3. funcții noi și îmbunătățiri; 9.6.4. probleme rezolvate; 9.6.5. probleme cunoscute. 9.7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului anti-malware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizări de produs: 9.8. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei 9.9. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 9.10. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. 9.11. Soluția include modulul de patch management și oferă posibilitatea de actualizare a aplicațiilor învechite instalate pe stațiile de lucru. **10. Certificate:** 10.1. Accesul la consola de management este doar prin HTTPS. 10.2. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitenta, data eliberării și data expirării certificatelor eliberate. **11. Caracteristici generale:** 11.1. Pentru reducerea la minim a consumului de resurse, soluția anti-malware permite instalarea personalizată a modulelor deținute (permite instalarea soluției anti- malware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 11.2. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva

		împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 11.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Anti-malware. 11.4. Pentru o mai bună protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționale). **12. Cerințe de sistem:** 12.1. Sisteme de operare pentru stații de lucru si servere: • Microsoft Windows 11 Enterprise LTSC / IoT Enterprise LTSC version 24H2; • Microsoft Windows 11 (all 64-bit editions, including ARM64); • Microsoft Windows 10 Enterprise LTSC / IoT Enterprise LTSC versions 2016, 2019 or 2021; • Microsoft Windows 10 (all 32-bit and 64-bit editions), ARM-based tablets are not supported; • Microsoft® Windows Server 2016 Standard; • Microsoft® Windows Server 2016 Essentials; • Microsoft® Windows Server 2016 Datacenter; • Microsoft® Windows Server 2016 Core; • Microsoft® Windows Server 2019 Standard; • Microsoft® Windows Server 2019 Datacenter; • Microsoft® Windows Server 2019 Core; • Microsoft® Windows Server 2022 Standard; • Microsoft® Windows Server 2022 Datacenter; • Microsoft® Windows Server 2022 Core; • Microsoft® Windows Server 2025 Standard; • Microsoft® Windows Server 2025 Datacenter; • Microsoft® Windows Server 2025 Core.	tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 11.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Anti-malware. 11.4. Pentru o mai bună protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționale). **12. Cerințe de sistem:** 12.1. Sisteme de operare pentru stații de lucru si servere: • Microsoft Windows 11 Enterprise LTSC / IoT Enterprise LTSC version 24H2; • Microsoft Windows 11 (all 64-bit editions, including ARM64); • Microsoft Windows 10 Enterprise LTSC / IoT Enterprise LTSC versions 2016, 2019 or 2021; • Microsoft Windows 10 (all 32-bit and 64-bit editions), ARM-based tablets are not supported; • Microsoft® Windows Server 2016 Standard; • Microsoft® Windows Server 2016 Essentials; • Microsoft® Windows Server 2016 Datacenter; • Microsoft® Windows Server 2016 Core; • Microsoft® Windows Server 2019 Standard; • Microsoft® Windows Server 2019 Datacenter; • Microsoft® Windows Server 2019 Core; • Microsoft® Windows Server 2022 Standard; • Microsoft® Windows Server 2022 Datacenter; • Microsoft® Windows Server 2022 Core; • Microsoft® Windows Server 2025 Standard; • Microsoft® Windows Server 2025 Datacenter; • Microsoft® Windows Server 2025 Core.

		12.2. Sisteme de operare linux pe baza distribuțiilor pe 64 de biți (AMD64/EM64T): • AlmaLinux 8, 9; • Amazon Linux 2; • Debian 10, 11, 12; • Oracle Linux 8, 9; • RHEL 8, 9; • Rocky Linux 8, 9; • SUSE Linux Enterprise Server 12 (Service Pack 5); • SUSE Linux Enterprise Server 15 (Service Pack 2 or newer); • Ubuntu 18.04, 20.04, 22.04, 24.04. 12.3. Sisteme de operare Security-Enhanced Linux cu urmatoarele distribuții: • Alma Linux 8, 9; • CentOS 7; • CentOS Stream 8; • Debian 10, 11, 12; • Oracle Linux 7, 8, 9; • RHEL 7, 8, 9; • Rocky Linux 8, 9. 12.4. Sisteme de operare macOS: • macOS 26 "Tahoe"; • macOS 15 "Sequoia"; • macOS 14 "Sonoma". **13. Administrare și instalare de la distanță:** 13.1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, browsing protection, device control, software update, application control, network location settings, automated tasks, dataguard (sandbox). 13.2. Instalarea se va putea face în mai multe moduri:	12.2. Sisteme de operare linux pe baza distribuțiilor pe 64 de biți (AMD64/EM64T): • AlmaLinux 8, 9; • Amazon Linux 2; • Debian 10, 11, 12; • Oracle Linux 8, 9; • RHEL 8, 9; • Rocky Linux 8, 9; • SUSE Linux Enterprise Server 12 (Service Pack 5); • SUSE Linux Enterprise Server 15 (Service Pack 2 or newer); • Ubuntu 18.04, 20.04, 22.04, 24.04. 12.3. Sisteme de operare Security-Enhanced Linux cu urmatoarele distribuții: • Alma Linux 8, 9; • CentOS 7; • CentOS Stream 8; • Debian 10, 11, 12; • Oracle Linux 7, 8, 9; • RHEL 7, 8, 9; • Rocky Linux 8, 9. 12.4. Sisteme de operare macOS: • macOS 26 "Tahoe"; • macOS 15 "Sequoia"; • macOS 14 "Sonoma". **13. Administrare și instalare de la distanță:** 13.1. Înainte de instalare, administratorul va particulariza pachetele de instalare cu modulele dorite: firewall, browsing protection, device control, software update, application control, network location settings, automated tasks, dataguard (sandbox). 13.2. Instalarea se va putea face în mai multe moduri:

		13.2.1. prin descărcarea directa a pachetului pe stația pe care se va face instalarea; 13.2.2. prin instalarea la distanta, direct din consola de management. 13.3. In consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc. 13.4. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe stații/servere. 13.5. Consola va include o secțiune, „Audit", unde se vor menționa toate acțiunile întreprinse in politica de securitate cu informații detaliate: logare, editare, creare etc. **14. Caracteristici și funcționalități principale ale modulului Anti-Malware și Endpoint Detection & Response (EDR)** 14.1. Soluția permite administratorului să stabilească acțiunea luata de produsul Anti-malware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni: 14.1.1. Acțiune implicită pentru fișiere infectate: 14.1.1.1. interzice accesul; 14.1.1.2. dezinfectează; 14.1.1.3. ștergere; 14.1.1.4. muta fișierele în carantină; 14.1.1.5. nicio acțiune; 14.1.2. Acțiune alternativa pentru fișierele infectate: 14.1.2.1. interzice accesul; 14.1.2.2. dezinfectează; 14.1.2.3. ștergere; 14.1.2.4. muta fișierele în carantină. 14.1.3. Acțiune implicită pentru fișierele suspecte: 14.1.3.1. interzice accesul; 14.1.3.2. ștergere; 14.1.3.3. muta fișierele în carantină;	13.2.1. prin descărcarea directa a pachetului pe stația pe care se va face instalarea; 13.2.2. prin instalarea la distanta, direct din consola de management. 13.3. In consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc. 13.4. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe stații/servere. 13.5. Consola include o secțiune, „Audit", unde se vor menționa toate acțiunile întreprinse in politica de securitate cu informații detaliate: logare, editare, creare etc. **14. Caracteristici și funcționalități principale ale modulului Anti-Malware și Endpoint Detection & Response (EDR)** 14.1. Soluția permite administratorului să stabilească acțiunea luata de produsul Anti-malware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni: 14.1.1. Acțiune implicită pentru fișiere infectate: 14.1.1.1. interzice accesul; 14.1.1.2. dezinfectează; 14.1.1.3. ștergere; 14.1.1.4. muta fișierele în carantină; 14.1.1.5. nicio acțiune; 14.1.2. Acțiune alternativa pentru fișierele infectate: 14.1.2.1. interzice accesul; 14.1.2.2. dezinfectează; 14.1.2.3. ștergere; 14.1.2.4. muta fișierele în carantină. 14.1.3. Acțiune implicită pentru fișierele suspecte: 14.1.3.1. interzice accesul; 14.1.3.2. ștergere; 14.1.3.3. muta fișierele în carantină;

		14.1.3.4. nicio acțiune; 14.1.4. Acțiune alternativa pentru fișierele suspecte: 14.1.4.1. interzice accesul; 14.1.4.2. ștergere; 14.1.4.3. muta fișierele în carantină. 14.2. Scanarea automată în timp real va putea fi setata să nu scaneze arhive. 14.3. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă. 14.4. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). 14.5. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 14.6. Configurarea cailor ce urmează a fi scanate la cerere. 14.7. Clienții anti-malware pentru stațiile de lucru să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese. 14.8. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware. 14.9. Posibilitatea de configura scanările programate să se execute cu prioritate redusă. 14.10. Pentru o protecție sporită, soluția anti-malware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazata pe monitorizarea proceselor. 14.11. Pentru o protecție sporită, soluția anti-malware trebuie să poată scana paginile HTTP. 14.12. Pentru o mai buna gestionare a anti-malware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare. 14.13. Pentru siguranța utilizatorului, clientul va include un modul de anti-phishing.	14.1.3.4. nicio acțiune; 14.1.4. Acțiune alternativa pentru fișierele suspecte: 14.1.4.1. interzice accesul; 14.1.4.2. ștergere; 14.1.4.3. muta fișierele în carantină. 14.2. Scanarea automată în timp real va putea fi setata să nu scaneze arhive. 14.3. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă. 14.4. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). 14.5. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 14.6. Configurarea cailor ce urmează a fi scanate la cerere. 14.7. Clienții anti-malware pentru stațiile de lucru să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese. 14.8. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware. 14.9. Posibilitatea de configura scanările programate să se execute cu prioritate redusă. 14.10. Pentru o protecție sporită, soluția anti-malware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazata pe monitorizarea proceselor. 14.11. Pentru o protecție sporită, soluția anti-malware trebuie să poată scana paginile HTTP. 14.12. Pentru o mai buna gestionare a anti-malware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare. 14.13. Pentru siguranța utilizatorului, clientul va include un modul de anti-phishing.

		14.14. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. 14.15. Soluția trebuie să permită instalarea serverelor de scanare externalizată în locația organizației, configurarea clienților pentru utilizarea acestora fără instalarea bazelor de date locale, trimiterea fișierelor necunoscute către serverele de scanare externalizată definite, optimizarea resurselor prin economisirea lățimii de bandă, procesării CPU și I/O-ului pe hard disk la nivelul endpoint-urilor, fără a afecta semnificativ performanța scanării fișierelor necunoscute, și să includă documentație detaliată privind funcționalitatea și implementarea. 14.16. Soluția trebuie să includă un modul de criptare la nivel de dispozitiv, care să asigure protecția confidențialității datelor stocate pe stații și laptopuri. Modulul de criptare trebuie să ofere: 14.16.1. Afișarea statusului de criptare pentru fiecare dispozitiv în consola de management. 14.16.2. Rapoarte dedicate și vizualizări de conformitate privind starea criptării la nivelul parcului IT. 14.16.3. Criptarea automată a disk-urilor pentru a preveni accesul neautorizat la informații sensibile în situații de pierdere, furt sau compromitere a dispozitivului. 14.16.4. Soluția trebuie să permită colectarea, stocarea și vizualizarea centralizată a cheilor de recuperare, pentru a facilita accesul legal în situații de blocare, restaurare sau migrare a datelor. 14.16.5. Funcția de colectare a cheilor trebuie să fie configurabilă din zona de profiluri a consolei de management. 14.17. Soluția trebuie să includă un sistem de protecție a folderelor sensibile, care să blocheze modificarea fișierelor de către aplicații necunoscute sau suspecte. Funcția trebuie să: 14.17.1. monitorizeze automat directoarele cu conținut utilizator (documente, fișiere de lucru etc.);	14.14. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. 14.15. Soluția trebuie să permită instalarea serverelor de scanare externalizată în locația organizației, configurarea clienților pentru utilizarea acestora fără instalarea bazelor de date locale, trimiterea fișierelor necunoscute către serverele de scanare externalizată definite, optimizarea resurselor prin economisirea lățimii de bandă, procesării CPU și I/O-ului pe hard disk la nivelul endpoint-urilor, fără a afecta semnificativ performanța scanării fișierelor necunoscute, și să includă documentație detaliată privind funcționalitatea și implementarea. 14.16. Soluția include un modul de criptare la nivel de dispozitiv, care să asigure protecția confidențialității datelor stocate pe stații și laptopuri. Modulul de criptare trebuie să ofere: 14.16.1. Afișarea statusului de criptare pentru fiecare dispozitiv în consola de management. 14.16.2. Rapoarte dedicate și vizualizări de conformitate privind starea criptării la nivelul parcului IT. 14.16.3. Criptarea automată a disk-urilor pentru a preveni accesul neautorizat la informații sensibile în situații de pierdere, furt sau compromitere a dispozitivului. 14.16.4. Soluția permite colectarea, stocarea și vizualizarea centralizată a cheilor de recuperare, pentru a facilita accesul legal în situații de blocare, restaurare sau migrare a datelor. 14.16.5. Funcția de colectare a cheilor este configurabilă din zona de profiluri a consolei de management. 14.17. Soluția include un sistem de protecție a folderelor sensibile, care să blocheze modificarea fișierelor de către aplicații necunoscute sau suspecte. Funcția face ca sa: 14.17.1. monitorizeze automat directoarele cu conținut utilizator (documente, fișiere de lucru etc.);

		14.17.2. permită accesul doar aplicațiilor de încredere, cu posibilitatea adăugării de excepții; 14.17.3. asigure protecție suplimentară împotriva atacurilor ransomware, chiar dacă alte straturi de securitate sunt evitate; 14.18. Soluția trebuie să includă un modul de Endpoint Detection and Response (EDR) integrat în același agent de protecție antivirus, fără instalări suplimentare. 14.19. Modulul EDR ar trebui să fie compatibil cu alți furnizori third party 14.20. Modulul EDR ar trebui să prezinte detecțiile sale, oferind ca informații cel puțin data și ora incidentului, nivelul de risc, gazdele afectate și contextul. EDR ar trebui să utilizeze o bază de cunoștințe disponibilă la nivel global, cum ar fi MITRE ATT&CK, pentru a oferi informații suplimentare și context atunci când este posibil. 14.21. Modulul EDR ar trebui să includă o caracteristică opțională, pentru a permite un contact rapid între client și echipa de analiză a amenințărilor OEM. Echipa OEM Threat Analysis ar trebui, în cazul în care este contactată de client, să efectueze o analiză detaliată cu privire la o anumită detecție pe EDR, ajutând clientul să confirme un posibil incident. Acest serviciu ar trebui să fie disponibil 27x7 pentru client 14.22. Modulul EDR ar trebui să verifice hashe-urile în bazele de date publice malware, cum ar fi VirusTotal, pentru a permite verificări la mai mulți furnizori AV 14.23. Modulul EDR trebuie să monitorizeze aplicațiile care rulează pe dispozitive și să semnaleze orice aplicații suspecte sau rău intenționate 14.24. EDR-ul trebuie activat într-un mod simplu, fără a necesita alte instalații 14.25. Modulul EDR trebuie sa ofere alertarea pe email 14.26. Modulul EDR trebuie sa ofere crearea rapoartelor cu o frecventa specificata. 14.27. Modulul EDR trebuie sa ofere posibilitatea de a crea task-uri ca de exemplu: Delete files, Delete registry, Delete scheduled tasks,	14.17.2. permită accesul doar aplicațiilor de încredere, cu posibilitatea adăugării de excepții; 14.17.3. asigure protecție suplimentară împotriva atacurilor ransomware, chiar dacă alte straturi de securitate sunt evitate; 14.18. Soluția include un modul de Endpoint Detection and Response (EDR) integrat în același agent de protecție antivirus, fără instalări suplimentare. 14.19. Modulul EDR este compatibil cu alți furnizori third party 14.20. Modulul EDR prezinta detecțiile sale, oferind ca informații cel puțin data și ora incidentului, nivelul de risc, gazdele afectate și contextul. EDR ar trebui să utilizeze o bază de cunoștințe disponibilă la nivel global, cum ar fi MITRE ATT&CK, pentru a oferi informații suplimentare și context atunci când este posibil. 14.21. Modulul EDR include o caracteristică opțională, pentru a permite un contact rapid între client și echipa de analiză a amenințărilor OEM. Echipa OEM Threat Analysis asigura, în cazul în care este contactată de client, să efectueze o analiză detaliată cu privire la o anumită detecție pe EDR, ajutând clientul să confirme un posibil incident. Acest serviciu este disponibil 27x7 pentru client 14.22. Modulul EDR verifica hashe-urile în bazele de date publice malware, cum ar fi VirusTotal, pentru a permite verificări la mai mulți furnizori AV 14.23. Modulul EDR monitorizeaza aplicațiile care rulează pe dispozitive și semnaleaza orice aplicații suspecte sau rău intenționate 14.24. EDR-ul se activeaza într-un mod simplu, fără a necesita alte instalații 14.25. Modulul EDR ofera alertarea pe email 14.26. Modulul EDR ofera crearea rapoartelor cu o frecventa specificata. 14.27. Modulul EDR ofera posibilitatea de a crea task-uri ca de exemplu: Delete files, Delete registry, Delete scheduled tasks, Delete

		Delete services, Enumerate processes, Enumerate services, Enumerate scheduled tasks, Full memory dump, Kill Process (Windows), Kill thread, Map registry, Map file system, Netstat, Process memory dump – Windows, Retrieve event log entries, Retrieve event log files, Retrieve files, Retrieve MBR, Retrieve MFT, Retrieve PowerShell history, Retrieve registry hives, Retrieve anti-virus logs, Enumerate WMI persistence, Delete WMI persistence, Retrieve browser artefacts. 14.28. Modulul EDR trebuie sa contina informatia legat de detectiile regasite pe dispozitiv in forma de rezumat, arborele de procese, analiza, log-uri. **15. Firewall:** 15.1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 15.2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 15.3. Posibilitatea de a defini rețele de încredere pentru mașina destinație. **16. Carantină:** 16.1. Produsul anti-malware să permită trimiterea automată a fișierelor din carantină către laboratoarele anti-malware ale producătorului. 16.2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator. 16.3. Produsul anti-malware să permită ștergerea automată a fișierelor din carantină mai vechi de o anumita perioadă, pentru a nu încărca inutil spațiul de stocare. 16.4. Posibilitatea de a restaura un fișier din carantină în locația lui originala. 16.5. Modulul de carantină va permite re-scanarea obiectelor după fiecare actualizare de semnături.	services, Enumerate processes, Enumerate services, Enumerate scheduled tasks, Full memory dump, Kill Process (Windows), Kill thread, Map registry, Map file system, Netstat, Process memory dump – Windows, Retrieve event log entries, Retrieve event log files, Retrieve files, Retrieve MBR, Retrieve MFT, Retrieve PowerShell history, Retrieve registry hives, Retrieve anti-virus logs, Enumerate WMI persistence, Delete WMI persistence, Retrieve browser artefacts. 14.28. Modulul EDR contine informatia legat de detectiile regasite pe dispozitiv in forma de rezumat, arborele de procese, analiza, log-uri. **15. Firewall:** 15.1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 15.2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 15.3. Posibilitatea de a defini rețele de încredere pentru mașina destinație. **16. Carantină:** 16.1. Produsul anti-malware permite trimiterea automată a fișierelor din carantină către laboratoarele anti-malware ale producătorului. 16.2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator. 16.3. Produsul anti-malware permite ștergerea automată a fișierelor din carantină mai vechi de o anumita perioadă, pentru a nu încărca inutil spațiul de stocare. 16.4. Posibilitatea de a restaura un fișier din carantină în locația lui originala. 16.5. Modulul de carantină va permite re-scanarea obiectelor după fiecare actualizare de semnături.

		17. Protecția datelor: 17.1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **18. Controlul conținutului:** 18.1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularități: 18.1.1. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. 18.1.2. Permite controlul accesului numai la anumite pagini de Internet specificate de administrator; 18.1.3. Permite blocarea accesului la anumite aplicații definite de administrator; 18.1.4. Permite restricționarea accesului pe anumite pagini de Internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). **19. Controlul aplicațiilor:** 19.1. Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, soluția permite definirea unor programe de actualizare (Updater) care vor fi lăsate să actualizeze diferite aplicații instalate pe stații sau servere. 19.2. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv sub procese) după: 19.2.1. Target path; 19.2.2. Target SHA 1; 19.2.3. Target SHA256; 19.2.4. Target file size; 19.2.5. Target signer name;	**17. Protecția datelor:** 17.1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **18. Controlul conținutului:** 18.1. Consola are integrat un modul dedicat controlului accesului la Internet cu următoarele particularități: 18.1.1. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. 18.1.2. Permite controlul accesului numai la anumite pagini de Internet specificate de administrator; 18.1.3. Permite blocarea accesului la anumite aplicații definite de administrator; 18.1.4. Permite restricționarea accesului pe anumite pagini de Internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). **19. Controlul aplicațiilor:** 19.1. Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, soluția permite definirea unor programe de actualizare (Updater) care vor fi lăsate să actualizeze diferite aplicații instalate pe stații sau servere. 19.2. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv sub procese) după: 19.2.1. Target path; 19.2.2. Target SHA 1; 19.2.3. Target SHA256; 19.2.4. Target file size; 19.2.5. Target signer name;

		19.2.6. Target certificate hash; 19.2.7. Target has trusted signature; 19.2.8. Parent path; 19.2.9. Parent signer name; 19.2.10. Parent certificate hash; 19.2.11. Parent has trusted signature. **20. Controlul dispozitivelor:** 20.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 20.2. Modulul va permite controlul următoarelor tipuri de dispozitive: 20.2.1. USB Mass Storage Device; 20.2.2. Wireless devices; 20.2.3. DVD/SC-ROM drivers; 20.2.4. Windows CE ActiveSync devices; 20.2.5. Floppy drivers; 20.2.6. Modems; 20.2.7. COM & LTP ports; 20.2.8. Printers; 20.2.9. Smart Card Readers; 20.2.10. Imaging Device (cameras and scanners) 20.2.11. IEEE 1394 Host Bus Controllers 20.2.12. IrDA Devices 20.2.13. Bluetooth Devices 20.3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client. 20.4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s- au configurat reguli. 20.5. Modulul va permite/bloca accesul pentru înscriere si rularea executabil. **21. Actualizare:**	19.2.6. Target certificate hash; 19.2.7. Target has trusted signature; 19.2.8. Parent path; 19.2.9. Parent signer name; 19.2.10. Parent certificate hash; 19.2.11. Parent has trusted signature. **20. Controlul dispozitivelor:** 20.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 20.2. Modulul permite controlul următoarelor tipuri de dispozitive: 20.2.1. USB Mass Storage Device; 20.2.2. Wireless devices; 20.2.3. DVD/SC-ROM drivers; 20.2.4. Windows CE ActiveSync devices; 20.2.5. Floppy drivers; 20.2.6. Modems; 20.2.7. COM & LTP ports; 20.2.8. Printers; 20.2.9. Smart Card Readers; 20.2.10. Imaging Device (cameras and scanners) 20.2.11. IEEE 1394 Host Bus Controllers 20.2.12. IrDA Devices 20.2.13. Bluetooth Devices 20.3. Modulul permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client. 20.4. Modulul permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s- au configurat reguli. 20.5. Modulul permite/bloca accesul pentru înscriere si rularea executabil. **21. Actualizare:**

		21.1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare).	21.1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare).
		CERINȚE FAȚĂ DE SERVICIILE DE IMPLEMENTARE și CONFIGURARE	**CERINȚE FAȚĂ DE SERVICIILE DE IMPLEMENTARE și CONFIGURARE**
		23. Caracteristici generale:	**23. Caracteristici generale:**
		23.1. Ofertantul selectat va livra și instala licențele pentru soluția ofertată. 23.2. Ofertantul selectat va efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a soluției aplicative în mediul de producție și mediul de testare. 23.3. Ofertantul selectat va efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială se înțelege setarea tuturor parametrilor aplicabili în corespundere cu cerințele (clientului), inclusiv configurarea și instalarea soluției ofertate, setarea politicilor și testarea înainte de a fi pusa în producție. 23.4. în baza rezultatelor de la etapa de design. Ofertantul selectat va implementa toate configurările / customizările agreate și darea în exploatare a soluției. 23.5. Ofertantul selectat va efectua instalarea soluției ofertate în întreaga infrastructură, inclusiv la toți utilizatorii finali (instalarea se va considera încheiată în momentul când toți utilizatorii vor avea instalat agentul și calculatorul va primi cel puțin o actualizare a bazelor și a agentului). 23.6. La sfârșitul etapei. Ofertantul va face o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare. 23.7. După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție post- implementare și suport. Perioada de	23.1. SC Xontech Systems SRL va livra și instala licențele pentru soluția ofertată. 23.2. SC Xontech Systems SRL va efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a soluției aplicative în mediul de producție și mediul de testare. 23.3. SC Xontech Systems SRL va efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială se înțelege setarea tuturor parametrilor aplicabili în corespundere cu cerințele (clientului), inclusiv configurarea și instalarea soluției ofertate, setarea politicilor și testarea înainte de a fi pusa în producție. 23.4. în baza rezultatelor de la etapa de design. SC Xontech Systems SRL va implementa toate configurările / customizările agreate și darea în exploatare a soluției. 23.5. SC Xontech Systems SRL va efectua instalarea soluției ofertate în întreaga infrastructură, inclusiv la toți utilizatorii finali (instalarea se va considera încheiată în momentul când toți utilizatorii vor avea instalat agentul și calculatorul va primi cel puțin o actualizare a bazelor și a agentului). 23.6. La sfârșitul etapei. SC Xontech Systems SRL va face o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare. 23.7. După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție post- implementare și suport. Perioada de garanție

		garanție post-implementare și suport va fi de 1 an calendaristic de la data activării acestei opțiuni. 23.8. Serviciile de garanție post-implementare și suport se referă la serviciile oferite de către Ofertantul selectat adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor. 23.9. Serviciile de garanție post-implementare și suport, vor include următoarele componente: 23.9.1. Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de producător; 23.9.2. Gestionarea incidentelor de securitate apărute pe perioada suportului activ; 23.9.4. Solicitări de analiza și corecție a politicilor de securitate în cadrul companiei implementate. **24. Cerințele față de serviciile de instruire** 24.1. În cadrul proiectului, Ofertantul va organiza sesiuni de instruire și transfer de cunoștințe pentru grupurile țintă în vederea formării setului de cunoștințe necesar pentru a permite echipei instruite să preia menținerea și configurarea ulterioară a soluției, în conformitate cu necesitățile utilizatorilor. 24.2. Instruirea se va organiza pentru diferite grupuri țintă la sediul Cumpărătorului. 24.3. Administrator - 2 persoane. 24.4. în acest sens, Ofertantul va prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruiri va efectua Ofertantul, pentru ce categorie de utilizatori, precum și cuprinsul/agenda acestor instruiri. 24.5. în afara instruirilor ce țin de utilizarea soluției, Ofertantul trebuie să efectueze și sesiuni de instruire pentru echipa de mentenanță din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoștințe și competențe, pentru a putea utiliza eficient	post-implementare și suport va fi conform termenul ofertat si ca prelungire a subscriptiei existente. 23.8. Serviciile de garanție post-implementare și suport se referă la serviciile oferite de către SC Xontech Systems SRL adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor. 23.9. Serviciile de garanție post-implementare și suport, vor include următoarele componente: 23.9.1. Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de producător; 23.9.2. Gestionarea incidentelor de securitate apărute pe perioada suportului activ; 23.9.4. Solicitări de analiza și corecție a politicilor de securitate în cadrul companiei implementate. **24. Cerințele față de serviciile de instruire** 24.1. În cadrul proiectului, SC Xontech Systems SRL va organiza sesiuni de instruire și transfer de cunoștințe pentru grupurile țintă în vederea formării setului de cunoștințe necesar pentru a permite echipei instruite să preia menținerea și configurarea ulterioară a soluției, în conformitate cu necesitățile utilizatorilor. 24.2. Instruirea se va organiza pentru diferite grupuri țintă la sediul Cumpărătorului. 24.3. Administrator - 2 persoane. 24.4. Avind in vedere ca se ofera aceiasi solutie de la acelasi producator în acest sens, la necesitate de va prezenta un plan de instruire, precum și cuprinsul acestor instruiri, care se va completa si defini în coordonare cu Cumpărătorul reieșind din necesitățile interne a instituției. 24.5. în afara instruirilor ce țin de utilizarea soluției, SC Xontech Systems SRL va efectua și sesiuni de instruire pentru echipa de mentenanță din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoștințe și competențe, pentru a putea utiliza eficient

		instrumentele de configurare și dezvoltare disponibile în cadrul soluției. 24.6. în cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoștințe către echipa Cumpărătorului, Ofertantul va fi de acord ca cel puțin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părți. 24.7. Ofertantul selectat la etapa de încheiere a contractului, va trebui să elaboreze și să convină cu Cumpărătorul următoarele elemente ale componentei de instruire: 24.7.1. Strategia Ofertantului cu privire la instruire și programul de formare; 24.7.2. Structura și componența pachetului de cursuri pentru formare și a manualelor de studiu pentru fiecare categorie de utilizator; 24.7.3. Metodologia și procedurile de evaluare și control al eficienței și suficienței sesiunilor de instruire. 24.8. în cadrul sesiunilor de instruire, Ofertantul va pune la dispoziția Cumpărătorului întreg setul de documentație al soluției care să cuprindă cel puțin următoarele componente: 24.8.1. Ghidurile administratorilor; 24.8.2. Ghidurile de instalare și configurare; 24.8.3. Fișierele surse pentru toate configurările și customizările realizate pe parcursul proiectului. **25. Licențe:** 25.1. Licente pentru 100 stații de lucru fizice/virtualizat. 25.2. Licente pentru 5 servere fizice/virtualizate.	instrumentele de configurare și dezvoltare disponibile în cadrul soluției. 24.6. în cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoștințe către echipa Cumpărătorului, SC Xontech Systems SRL este de acord ca cel puțin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părți. 24.7. SC Xontech Systems SRL la etapa de încheiere a contractului, va elabora și va conveni cu Cumpărătorul următoarele elemente ale componentei de instruire: 24.7.1. Strategia Ofertantului cu privire la instruire și programul de formare; 24.7.2. Structura și componența pachetului de cursuri pentru formare și a manualelor de studiu pentru fiecare categorie de utilizator; 24.7.3. Metodologia și procedurile de evaluare și control al eficienței și suficienței sesiunilor de instruire. 24.8. în cadrul sesiunilor de instruire, SC Xontech Systems SRL va pune la dispoziția Cumpărătorului întreg setul de documentație al soluției care cuprinde cel puțin următoarele componente: 24.8.1. Ghidurile administratorilor; 24.8.2. Ghidurile de instalare și configurare; 24.8.3. Fișierele surse pentru toate configurările și customizările realizate pe parcursul proiectului. **25. Licențe:** 25.1. Licente pentru 100 stații de lucru fizice/virtualizat. 25.2. Licente pentru 5 servere fizice/virtualizate.