

Anexa nr.1
la Caietul de sarcini

Specificații tehnice

Numărul procedurii de achiziție: **ocds-b3wdp1-MD-1733471227814**

Obiectul achiziției: **Pachete software aferente securității informaționale**

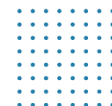
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
Soluție de protecție, securitate și criptare pentru stații de lucru	Bitdefender GravityZone Business Security Enterprise	România	Bitdefender	<p>Tip: Subscriere anuală pentru soluția de protecție și securitate pentru 914 entități (PC/ laptop/ VDI/ Server) pentru perioada 12.01.2025-12.01.2026.</p> <p>Cantitate: Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul:</p> <ul style="list-style-type: none"> - 914 entități (PC/laptop/VDI/Server) - Disk Encryption management pentru 543 entități. <p>Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări „AV-TEST”, „VIRUS BULLETIN'S”, „REAL-WORLD PROTECTION”, „MALWARE PROTECTION”).</p> <p>Specificații tehnice: Soluția va acoperi minim următoarele cerințe și specificații tehnice: <i>Caracteristici generale ale produsului:</i> Soluția trebuie să reprezinte o platformă integrată pentru managementul securității, gândita ca o soluție modulară. Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:</p> <ul style="list-style-type: none"> - Protecție stații și servere fizice și virtualizate; - Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android; - Serviciu de corelare și răspuns la evenimente de tip EDR („endpoint detection and response”). <p><i>Consola de management:</i> Accesibilitate atât de pe browser desktop cât și tip mobile.</p>	<p>Tip: Subscriere anuală pentru soluția de protecție și securitate pentru 914 entități (PC/laptop/VDI/Server) pentru perioada 12.01.2025-12.01.2026.</p> <p>Cantitate: Se oferă soluția Bitdefender GravityZone, cu urmatorul model de licențiere:</p> <ul style="list-style-type: none"> - GravityZone Business Security Enterprise 914 entități (PC/laptop/VDI/Server); - GravityZone Full Disk Encryption Disk Encryption management pentru 543 entități. <p>Produsul antivirus oferit ocupă locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări „AV-TEST”, „VIRUS BULLETIN'S”, „REAL-WORLD PROTECTION”, „MALWARE PROTECTION”).</p> <p>Specificații tehnice: Soluția acoperă minim următoarele cerințe și specificații tehnice: <i>Caracteristici generale ale produsului:</i> Soluția reprezintă o platformă integrată pentru managementul securității, gândita ca o soluție modulară. Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:</p> <ul style="list-style-type: none"> - Protecție stații și servere fizice și virtualizate; - Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android; - Serviciu de corelare și răspuns la evenimente de tip EDR („endpoint detection and response”). <p>Consola de management: Accesibilă atât de pe browser desktop cât și tip mobile.</p>	





Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<p>Să ofere opțiuni configurabilă de actualizare automată a consolei de management.</p> <p><u>Soluția de scanare centralizată:</u> Soluția de scanare (pentru VDI/scanare centralizată) disponibilă de tip template și compatibilă cu următoarele hipervizoare::</p> <ol style="list-style-type: none"> 1) VMware vSphere; 2) Citrix XenServer; 3) Microsoft Hyper-V. <p><u>Cerințe generale produs:</u> Soluția trebuie să:</p> <ul style="list-style-type: none"> – permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; – ofere vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme rezolvate, probleme cunoscute; – afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile); <p><u>Panou de monitorizare și raportare (Dashboard):</u></p> <ul style="list-style-type: none"> – să ofere posibilitatea creării rapoartelor configurabile după tip, țintă și scop cu opțiuni specifice pentru orice tip de raport cu posibilități de adăugare/eliminare și rearanjare. – să prezinte rapoarte pentru toate modulele suportate(stare/statut/actualizare). <p><u>Inventarierea rețelei – managementul securității:</u> Produsul trebuie să:</p> <ul style="list-style-type: none"> – se integreze cu domenii Active Directory multiple, să poată importa inventarul. – permită descoperirea PC neintegrate în Active Directory (Workgroup); – ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP, politica aplicată, online și/sau offline și FQDN; 	<p>Oferă opțiuni configurabilă de actualizare automată a consolei de management.</p> <p><u>Soluția de scanare centralizată:</u> Soluția de scanare (pentru VDI/scanare centralizată) disponibilă de tip template și compatibilă cu următoarele hipervizoare::</p> <ol style="list-style-type: none"> 1) VMware vSphere; 2) Citrix XenServer; 3) Microsoft Hyper-V. <p><u>Cerințe generale produs:</u> Soluția:</p> <ul style="list-style-type: none"> – permite activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; – oferă vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme rezolvate, probleme cunoscute; – afișează notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile); <p><u>Panou de monitorizare și raportare (Dashboard):</u></p> <ul style="list-style-type: none"> – oferă posibilitatea creării rapoartelor configurabile după tip, țintă și scop cu opțiuni specifice pentru orice tip de raport cu posibilități de adăugare/eliminare și rearanjare. – prezintă rapoarte pentru toate modulele suportate(stare/statut/actualizare). <p><u>Inventarierea rețelei – managementul securității:</u> Produsul:</p> <ul style="list-style-type: none"> – se integrează cu domenii Active Directory multiple, poate importa inventarul. – permite descoperirea PC neintegrate în Active Directory (Workgroup); – oferă opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP, politica aplicată, online și/sau offline și FQDN; 	





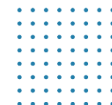
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<ul style="list-style-type: none"> - permite instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale; - permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale; - permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus; - oferă posibilitatea de repornire a mașinilor fizice de la distanță; - oferă informații detaliate despre fiecare task inițiat și afișarea statutului lui; - permite configurarea centralizată a clienților antivirus prin intermediul politicilor; - oferă în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături; - permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. <p><u>Politici:</u> Produsul trebuie să:</p> <ul style="list-style-type: none"> - permite configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module; - conține opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user; - permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy; - poate fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în 	<ul style="list-style-type: none"> - permite instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale; - permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale; - permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus; - oferă posibilitatea de repornire a mașinilor fizice de la distanță; - oferă informații detaliate despre fiecare task inițiat și afișarea statutului lui; - permite configurarea centralizată a clienților antivirus prin intermediul politicilor; - oferă în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături; - permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. <p><u>Politici:</u> Produsul:</p> <ul style="list-style-type: none"> - permite configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module; - conține opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user; - permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy; - poate fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în 	





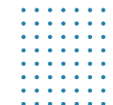
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<p>accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless).</p> <p><u>Monitorizare și raportare:</u> Produsul trebuie să:</p> <ul style="list-style-type: none"> - permită setarea de opțiuni specifice pentru afișarea rapoartelor existente; - dețină un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate; - conțină rapoarte care prezintă statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate; - trimită rapoarte către un număr nelimitat de adrese de email; - permită vizualizarea rapoartelor curente programate de administrator; - permită exportarea rapoartelor în format .pdf și detaliile ca format .csv; - includă un generator de rapoarte care să ofere posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal; - ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor; - ofere interogări legate de evenimente precum: calculatorul ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc); <p><u>Carantină:</u></p>	<p>accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless).</p> <p><u>Monitorizare și raportare:</u> Produsul:</p> <ul style="list-style-type: none"> - permite setarea de opțiuni specifice pentru afișarea rapoartelor existente; - deține un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate; - conține rapoarte care prezintă statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate; - trimite rapoarte către un număr nelimitat de adrese de email; - permite vizualizarea rapoartelor curente programate de administrator; - permite exportarea rapoartelor în format .pdf și detaliile ca format .csv; - include un generator de rapoarte care să ofere posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal; - oferă interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor; - oferă interogări legate de evenimente precum: calculatorul ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc); <p><u>Carantină:</u></p>	





Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<ul style="list-style-type: none"> - Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă; - Administrarea Carantinei să fie posibilă atât pe terminalul administrat cât și din consola de management; <p><u>Utilizatori:</u></p> <ul style="list-style-type: none"> - Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări; - Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management; - Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil. <p><u>Log-uri:</u></p> <ul style="list-style-type: none"> - Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. <p><u>Actualizare:</u> Soluția va permite:</p> <ul style="list-style-type: none"> - definirea de locații de actualizare multiple - activarea/dezactivarea actualizărilor - testarea noilor versiuni înainte de a fi instalate pe toți clienții (posibilitate de actualizare în mai multe cicluri - 1 mediu de test, 2 - mediu de producție) - definirea zonelor de test și zonelor critice de producție <p><u>Protecție stații și servere fizice și virtualizate - caracteristici minime:</u> Soluția trebuie să:</p>	<ul style="list-style-type: none"> - Produsul permite restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă; - Administrarea Carantinei este posibilă atât pe terminalul administrat cât și din consola de management; <p><u>Utilizatori:</u></p> <ul style="list-style-type: none"> - Administrarea este efectuată pe bază de roluri multiple predefinite : Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări; - Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management; - Este posibil deconectarea automată a oricărui tip de utilizator după un anumit timp. <p><u>Log-uri:</u></p> <ul style="list-style-type: none"> - Soluția permite înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. <p><u>Actualizare:</u> Soluția permite:</p> <ul style="list-style-type: none"> - definirea de locații de actualizare multiple - activarea/dezactivarea actualizărilor - testarea noilor versiuni înainte de a fi instalate pe toți clienții (posibilitate de actualizare în mai multe cicluri - 1 mediu de test, 2 - mediu de producție) - definirea zonelor de test și zonelor critice de producție <p><u>Protecție stații și servere fizice și virtualizate - caracteristici minime:</u> Soluția antivirus:</p>	





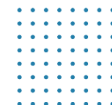
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<ul style="list-style-type: none"> - permită instalarea personalizată a modulelor; - includă un „vaccin” anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și blocarea procesului de criptare; - includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate); - includă modul de analiză la risk capabil să identifice și să remedieze riskurile identificate la nivel de rețea sau sistem de operare, cu posibilitate de configurare și automatizare; - includă modul avansat de securitate bazat pe tehnologii de tip „machine learning tunabil” proiectat special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție; - includă modul avansat de securitate pentru protecție împotriva: atacurilor direcționate (Targeted Attack), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv cu posibilitate de extindere a nivelului de raportare; - includă modul de sandbox, unde se vor putea trimite manual sau automat fișiere pentru a putea fi „detonate” pentru o analiză în profunzime; - includă variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acțiuni de remediere: implicită și de siguranță. Pentru acțiunea implicită: doar raportare, dezinfectie, ștergere și transmitere în carantină. Pentru acțiunea de siguranță: ștergere sau permutare în carantină; - suportă „detonarea” în modulul sandbox, minim, tipurile de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR 	<ul style="list-style-type: none"> - permite instalarea personalizată a modulelor; - include un „vaccin” anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și blocarea procesului de criptare; - include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate); - include modul de analiză la risk capabil să identifice și să remedieze riskurile identificate la nivel de rețea sau sistem de operare, cu posibilitate de configurare și automatizare; - include modul avansat de securitate bazat pe tehnologii de tip „machine learning tunabil” proiectat special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție; - include modul avansat de securitate pentru protecție împotriva: atacurilor direcționate (Targeted Attack), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, i se poate stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv cu posibilitate de extindere a nivelului de raportare; - include modul de sandbox, unde se poate trimite manual sau automat fișiere pentru a putea fi „detonate” pentru o analiză în profunzime; - include variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acțiuni de remediere: implicită și de siguranță. Pentru acțiunea implicită: doar raportare, dezinfectie, ștergere și transmitere în carantină. Pentru acțiunea de siguranță: ștergere sau permutare în carantină; - suportă „detonarea” în modulul sandbox, minim, tipurile de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR 	



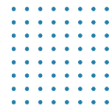


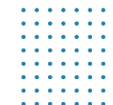
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<p>(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. Acestea vor fi detectate corect chiar dacă vor fi în arhive de tipul : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ ;</p> <ul style="list-style-type: none"> - ofere posibilitate de filtrare a incidentelor din interfața grafică în funcție intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cât și după IP, nume fișier, nume stație; - permită vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: să generează o hartă de principiu a incidentului, să detalieze incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod); - poată bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV; - poată excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase; - permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permită executarea 	<p>(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. Acestea vor fi detectate corect chiar dacă vor fi în arhive de tipul : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ ;</p> <ul style="list-style-type: none"> - oferă posibilitate de filtrare a incidentelor din interfața grafică în funcție intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cât și după IP, nume fișier, nume stație; - permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: care generează o hartă de principiu a incidentului, detaliază incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, poate genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod); - poate bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV; - poate excepta fișiere non-malițioase de la acțiunea de investigare sau generarea/ adăugarea un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase; - permite deschiderea unei conexiuni remote către un endpoint potențial infectat pentru o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permită executarea unor 	





Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<p>unor comenzi în linia de comandă care se execută cu privilegiul de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare;</p> <ul style="list-style-type: none"> - permită crearea regulilor de detecție personalizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; - permită crearea regulilor de excludere personalizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; - permită căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; - permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru investigare rapidă, colectare date și remedierea în timp real a breșei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegiul de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare - include modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response”) capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. Acest modul va fi capabil să : <ul style="list-style-type: none"> a) cuprindă colectarea de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate; b) oferă senzori de colectare a datelor și componente de procesare și interpretare a acestora; c) posedă capacitatea de evaluare a activității tipice a unui endpoint din perspectiva 	<p>comenzi în linia de comandă care se execută cu privilegiul de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare;</p> <ul style="list-style-type: none"> - permite crearea regulilor de detecție personalizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; - permite crearea regulilor de excludere personalizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; - permite căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; - permite deschiderea unei conexiuni remote către un endpoint potențial infectat pentru investigare rapidă, colectare date și remedierea în timp real a breșei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegiul de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare - include modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response”) capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. Acest modul este capabil să : <ul style="list-style-type: none"> a) cuprindă colectarea de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate; b) oferă senzori de colectare a datelor și componente de procesare și interpretare a acestora; c) posedă capacitatea de evaluare a activității tipice a unui endpoint din perspectiva 	





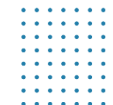
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<p>securității acestuia conform tehnicilor de atac MITRE („baselining”) și va raporta orice deviație de la acest comportament sub forma unui incident;</p> <p>d) oferă vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generând o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează” care poate genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);</p> <p>e) poate bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;</p> <p>f) poate excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase</p> <p>g) permite vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri.</p> <p><u>Cerințe de sistem:</u></p> <ul style="list-style-type: none"> – Sisteme de operare pentru stații de lucru: Windows 10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent; – Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022. <p><u>Administrare și instalare remote:</u></p>	<p>securității acestuia conform tehnicilor de atac MITRE („baselining”) și va raporta orice deviație de la acest comportament sub forma unui incident;</p> <p>d) oferă vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generând o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează” care poate genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);</p> <p>e) blochează fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;</p> <p>f) poate excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase</p> <p>g) permite vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri.</p> <p><u>Cerințe de sistem:</u></p> <ul style="list-style-type: none"> – Sisteme de operare pentru stații de lucru: Windows 10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent; – Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022. <p><u>Administrare și instalare remote:</u></p>	





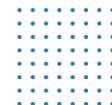
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<ul style="list-style-type: none"> - Pachetele de instalare trebuie să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay” (update server”); - Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management; - Din consola să fie disponibile informații despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări; - Posibilități de creare kit pentru endpoint – tip: universar – 32/64bit, fizic/VDI, web installe/full. - Gestionare, creare și configurare grupuri pentru endpoint ce nu sunt în AD; - Posibilitate de atribuire a funcționalității de descoperire a endpointurilor și în afara AD, pentru oricare endpoint. <p><u>Caracteristici și funcționalități principale ale modului antivirus:</u> Produsul trebuie sa permită:</p> <ul style="list-style-type: none"> - stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: <ol style="list-style-type: none"> a) implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune; b) alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină; c) acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune; d) acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină; - scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la 	<ul style="list-style-type: none"> - Pachetele de instalare sunt configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay” (update server”); - Există posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management; - Din consola este disponibilă informații despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări; - Există posibilități de creare kit pentru endpoint – tip: universar – 32/64bit, fizic/VDI, web installe/full. - Gestionare, creare și configurare grupuri pentru endpoint ce nu sunt în AD; - Există posibilitatea de atribuire a funcționalității de descoperire a endpointurilor și în afara AD, pentru oricare endpoint. <p><u>Caracteristici și funcționalități principale ale modului antivirus:</u> Produsul permite:</p> <ul style="list-style-type: none"> - stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: <ol style="list-style-type: none"> a) implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune; b) alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină; c) acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune; d) acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină; - scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la 	





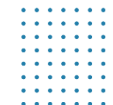
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<p>scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de " x" MB, definirea nivelelor de profunzime pentru scanarea în arhive;</p> <ul style="list-style-type: none"> - scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă; - scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc); - scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP; - configurarea căilor ce urmează a fi scanate la cerere; - 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; - setarea priorităților scanărilor programate; - configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware; - administratorului să personalizeze și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată în Cloud-ul privat, scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid; - setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor; - scanarea paginilor web; - setarea a unei parole pentru protecția la dezinstalare; 	<p>scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de «x» MB, definirea nivelelor de profunzime pentru scanarea în arhive;</p> <ul style="list-style-type: none"> - scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă; - scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc); - scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP; - configurarea căilor ce urmează a fi scanate la cerere; - 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; - setarea priorităților scanărilor programate; - configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware; - administratorului să personalizeze și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată în Cloud-ul privat, scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid; - setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor; - scanarea paginilor web; - setarea a unei parole pentru protecția la dezinstalare; 	





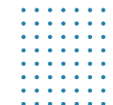
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<ul style="list-style-type: none"> - modul de antiphishing; - protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată; - instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale; - utilizarea unui modul adițional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze și blocheze atacuri de tip persistent sau targetat precum și alte categorii de malware sofisticat înainte de faza de execuție. Acest modul oferă următoarele funcționalități: <ul style="list-style-type: none"> a) clasificarea tipului de atac; b) abilitatea de a raporta amenințările detectate fără a le bloca; c) abilitate de a ajusta agresivitatea detecției pe cel puțin 3 nivele (incluzând posibilitatea de a raporta atacuri ce ar fi fost blocate pe un nivel de agresivitate a detecției „mai ridicat” decât cel setat în mod curent în modul); d) abilitatea de a acționa în mod diferit în funcție de tipul amenințării (fișier sau atac prin rețea); - posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, când determină că procesul este malițios; - oprirea atacurilor avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive; - depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare; - protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem” cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare. 	<ul style="list-style-type: none"> - modul de antiphishing; - protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată; - instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale; - utilizarea unui modul adițional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze și blocheze atacuri de tip persistent sau targetat precum și alte categorii de malware sofisticat înainte de faza de execuție. Acest modul oferă următoarele funcționalități: <ul style="list-style-type: none"> a) Clasificarea tipului de atac; b) Abilitatea de a raporta amenințările detectate fără a le bloca; c) Abilitate de a ajusta agresivitatea detecției pe cel puțin 3 nivele (incluzând posibilitatea de a raporta atacuri ce ar fi fost blocate pe un nivel de agresivitate a detecției „mai ridicat” decât cel setat în mod curent în modul); d) Abilitatea de a acționa în mod diferit în funcție de tipul amenințării (fișier sau atac prin rețea); - posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, când determină că procesul este malițios; - oprirea atacurilor avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive; - depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare; - protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem” cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare. 	



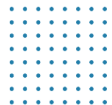


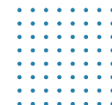
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<p><u>Firewall:</u></p> <ul style="list-style-type: none"> – sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; – modulul să poată fi instalat/ activat/ dezactivat/ deinstalat la cerere; – să permită definirea de rețele de încredere pentru mașina destinație. <p><u>Protecția datelor:</u></p> <ul style="list-style-type: none"> – Produsul trebuie să permită blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. <p><u>Controlul conținutului:</u></p> <p>Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violența, pornografia etc).</p> <p><u>Controlul dispozitivelor:</u></p> <p>Produsul trebuie să conțină un modul pentru controlul dispozitivelor care:</p> <ul style="list-style-type: none"> – poate fi instalat/deinstalat conform setărilor stabilite; – permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage; 	<p><u>Firewall:</u></p> <ul style="list-style-type: none"> – oferă posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; – modulul poate fi instalat/deinstalat la cerere; – permite definirea de rețele de încredere pentru mașina destinație; <p><u>Protecția datelor:</u></p> <ul style="list-style-type: none"> – Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. <p><u>Controlul conținutului:</u></p> <p>Produsul oferă un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violența, pornografia etc).</p> <p><u>Controlul dispozitivelor:</u></p> <p>Produsul conține un modul pentru controlul dispozitivelor care:</p> <ul style="list-style-type: none"> – poate fi instalat/deinstalat conform setărilor stabilite; – permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage; 	



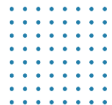


Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<ul style="list-style-type: none"> – permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client; – permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. <p><u>Power User:</u> Produsul trebuie să conțină un modul pentru setări specifice – power user care să:</p> <ul style="list-style-type: none"> – poată fi instalat/dezinstalat în funcție de preferința administratorului; – permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client; – permită administratorului soluției să suprascrise din consola setările aplicate de utilizatorii Power User. <p><u>Actualizare:</u> Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:</p> <ul style="list-style-type: none"> – la nivel de stație în mod silențios (fără avertizări); – folosind unul sau mai multe servere de actualizare; – pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare. – gestionabil – doar local sau și servere online. <p><u>Protecție Anti-Tampering:</u></p> <ul style="list-style-type: none"> – va permite detecția driverelor vulnerabile pe dispozitivele conectate (endpointuri) și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului; – va permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatare de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia este 	<ul style="list-style-type: none"> – permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client; – permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. <p>Power User: Produsul conține un modul pentru setări specifice – power user care:</p> <ul style="list-style-type: none"> – poate fi instalat/dezinstalat în funcție de preferința administratorului; – permite posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client; – permite administratorului soluției să suprascrise din consola setările aplicate de utilizatorii Power User. <p>Actualizare: Produsul oferă posibilitatea de efectuare a actualizărilor:</p> <ul style="list-style-type: none"> – la nivel de stație în mod silențios (fără avertizări); – folosind unul sau mai multe servere de actualizare; – pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare; – gestionabil – doar local sau și servere online. <p><u>Protecție Anti-Tampering:</u></p> <ul style="list-style-type: none"> – permite detecția driverelor vulnerabile pe dispozitivele conectate (endpointuri) și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului; – permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatare de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia este 	





Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referință
1	2	3	4	5	6	7
Lotul: Soluție de protecție, securitate și disk encryption						
				<p>compatibilă cu sistemele de operare Windows și Linux;</p> <ul style="list-style-type: none"> – va fi capabilă să protejeze împotriva amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios. <p><u>Disk Encryption:</u></p> <ul style="list-style-type: none"> – Soluție pentru managementul criptării discurilor pentru 543 calculatoare portabile. – Soluția va oferi următoarele funcționalități minime: – Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus; – produsul va utiliza mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows și FileVault pentru Mac OSX; – va asigura vizibilitatea completă asupra stării de criptare a dispozitivelor inclusiv: numele stației, IP-ul stației, sistemul de operare, ID-ul volumului/partiției, numele partiției, starea criptării partiției, tipul partiției: boot, non-boot, mărimea partiției în GB, ID-ul cheii de recuperare; – Produsul trebuie să asigure criptarea pentru Următoarele OS: Windows 10/11 Pro/Enterprise (with TPM); WindowsServer 2012/2012 R2, 2016, 2019, 2022 (with TPM), OSX de la 10.12. <p><u>Alte cerințe:</u></p> <p><u>Perioada de suport și mentinere de la producător:</u></p> <ol style="list-style-type: none"> 1) Pentru soluția oferită se solicită a fi 12 luni pentru perioada 12.01.2025-12.01.2026; 2) Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță. <p><u>Notă:</u> Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de</p>	<p>compatibilă cu sistemele de operare Windows și Linux;</p> <ul style="list-style-type: none"> – este capabilă să protejeze împotriva amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios. <p><u>Disk Encryption:</u></p> <ul style="list-style-type: none"> – Soluție pentru managementul criptării discurilor pentru 543 calculatoare portabile. – Soluția acoperă următoarele funcționalități minime: – Administrarea produsului este realizată din aceeași consolă de management ca și soluția de protecție antivirus; – produsul folosește mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows și FileVault pentru Mac OSX; – Produsul oferă un raport complet asupra stării de criptare a dispozitivelor inclusiv: numele stației, IP-ul stației, sistemul de operare, ID-ul volumului/partiției, numele partiției, starea criptării partiției, tipul partiției: boot, non-boot, mărimea partiției în GB, ID-ul cheii de recuperare; – Produsul asigură criptarea pentru următoarele OS: Windows 10/11 Pro/Enterprise (with TPM); WindowsServer 2012/2012 R2, 2016, 2019, 2022 (with TPM), OSX de la 10.12. <p><u>Alte cerințe:</u></p> <p><u>Perioada de suport și mentinere de la producător:</u></p> <ol style="list-style-type: none"> 1) Soluția oferită se va livra pentru 12 luni pentru perioada 12.01.2025-12.01.2026; 2) Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță. 	





„RTS ONE” S.R.L.



1018600009979



(+373) 22 101 777



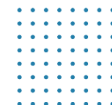
office@rts.one



http://rts.md



str. Mitropolit G. Bănulescu-Bodoni, 59/B, of.804



Denumirea bunurilor	Modelul articolului	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
Lotul: Soluție de protecție, securitate și disk encryption						
				Ofertant, iar costul acestora trebuie să fie incluse în ofertă (după caz).	<u>Notă:</u> Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi executate de Ofertant, iar costul acestora trebuie este inclus în ofertă.	
TOTAL						

Semnat:

Numele, Prenumele: **CELONENCO Vitalie**Ofertantul: **„RTS ONE” S.R.L.**În calitate de: **Administrator**Adresa: **mun.Chișinău, str.Mitropolit Gavriil Bănulescu-Bodoni, 59/B, of.804**