Specificații tehnice

Numărul procedurii de achiziție: MTender ID: **ocds-b3wdp1-MD-1698909671458 din 22 noiembrie 2023**
Obiectul achiziției: **Pachete software aferente securității informaționale**

Denumirea bunurilor	**Modelul articolului**	**Țara de origine**	**Producă-torul**	**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*
Soluție de protecție, securitate și disk encryption pentru locurile de muncă	Bitdefender GravityZone Business Security Enterprise, GravityZone Full Disk Encryption	România	Bitdefender	**Tip:** Subscriere anuală pentru soluția de protecție și securitate pentru 850 entități (PC/laptop/VDI/Server) pentru perioada 12.01.2024-12.01.2025. **Cantitate:** Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul: - 850 entități (PC/laptop/VDI/Server) și 700 căsuțe poștale; - Disk Encryption management pentru 353 entități. 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"). **Caracteristici generale ale produsului:** 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: • Protecție stații și servere fizice și virtualizate; • Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android; • Protecție și securitate pentru serverele email Microsoft Exchange; • Serviciu de corelare și răspuns la evenimente de tip EDR („endpoint detection and response"). **Consola de management:** Pachetul de instalare să fie livrat ca o mașină virtuală, care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare. Imaginea de tip template să poată a fi importa în:	**Tip:** Subscriere anuală pentru soluția de protecție și securitate pentru 850 entități (PC/laptop/VDI/Server) pentru perioada 12.01.2024-12.01.2025. **Cantitate:** Se oferă soluția Bitdefender GravityZone, cu urmatorul model de licentiere: - GravityZone Business Security Enterprise 850 entități (PC/laptop/VDI/Server) și 1270 căsuțe poștale; - GravityZone Full Disk Encryption Disk Encryption management pentru 353 entități. 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"). **Caracteristici generale ale produsului:** 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: • Protecție stații și servere fizice și virtualizate; • Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android; • Protecție și securitate pentru serverele email Microsoft Exchange; • Serviciu de corelare și răspuns la evenimente de tip EDR („endpoint detection and response"). **Consola de management:** Pachetul de instalare să fie livrat ca o mașină virtuală, care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare. Imaginea de tip template să poată a fi importa în:	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	*2*	*3*	*4*	*5*	*6*	*7*
				1. VMware vSphere; 2. Citrix XenServer; 3. Microsoft Hyper-V; 4. KVM; 5. Nutanix. Consola de management să fie livrată cu o baza de date inclusă, non-relațională fără a fi nevoie de licențe adiționale. Soluția trebuie să: • fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri; • asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web; • asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management; • includă un modul load balancer pentru performanța și redundanță; • includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering). **<u>Cerințe generale produs:</u>** Soluția trebuie să: 1. includă un unul sau mai multe module de update server prin care să asigure actualizarea componentelor și a semnăturilor; 2. permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; 3. transmită alerte de ne funcționalitate, cu 30 de minute înainte de actualizare; 4. permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute; 5. afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile);	1. VMware vSphere; 2. Citrix XenServer; 3. Microsoft Hyper-V; 4. KVM; 5. Nutanix. Consola de management va fi livrată cu o baza de date inclusă, non-relațională fără a fi nevoie de licențe adiționale. Soluția: • este scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri; • asigură următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web; • asigură posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management; • include un modul load balancer pentru performanța și redundanță; • include mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering). **<u>Cerințe generale produs:</u>** Soluția: 1. include un unul sau mai multe module de update server prin care să asigure actualizarea componentelor și a semnăturilor; 2. permite activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; 3. transmite alerte de ne funcționalitate, cu 30 de minute înainte de actualizare; 4. permite vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute; 5. afișează notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile);	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	*2*	*3*	*4*	*5*	*6*	*7*
				6. permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus; 7. permită instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management; 8. permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocata local, pe un server FTP sau în rețea. **Inventarierea rețelei – managementul securității:** Produsul trebuie să: - se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme; - permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM, Nutanix Prism; - permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery; - ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP; - permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale; - permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale; - permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus; - ofere posibilitatea de repornire a mașinilor fizice de la distanță; - ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui; - permită configurarea centralizată a clienților antivirus prin intermediul politicilor; - ofere 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; - permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.	6. permite integrarea cu un server Syslog pentru raportarea evenimentelor antivirus; 7. permite instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management; 8. permite crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocata local, pe un server FTP sau în rețea. **Inventarierea rețelei – managementul securității:** Produsul: - se integrează cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme; - permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM, Nutanix Prism; - permite descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery; - oferă opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP; - 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.	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				Politici: Produsul trebuie să: - permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module; - conțină 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; - permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy; - poată 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 accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless). **Monitorizare și raportare:** Produsul trebuie să: - 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 prezinta 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 si detaliile ca format .csv; - includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange;	**Politici:** Produsul: - 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 accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless). **Monitorizare și raportare:** Produsul: - 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 prezinta 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 si detaliile ca format .csv; - include un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange;	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	*2*	*3*	*4*	*5*	*6*	*7*
				- 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); - ofere interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau carantinarea fișierului, ștergerea sau respingerea e-mail-ului). **Carantină:** - Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă; - Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management; **Utilizatori:** - 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. **Log-uri:** - Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații	- 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); - oferă interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau carantinarea fișierului, ștergerea sau respingerea e-mail-ului). **Carantină:** - Produsul permite restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă; - Locația, fișierele și administrarea Carantinei este efectuată central din consola de management; **Utilizatori:** - 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. **Log-uri:** - Soluția permite înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. **<u>Protecție stații și servere fizice si virtualizate – caracteristici minime:</u>** Soluția antivirus trebuie să: - 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 daca sunt infectate și blocarea procesului de criptare; - includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate); - includă modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activitati suspecte în faza pre-executie; - includă modul avansat de securitate pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fisierelor suspecte si 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 includere în sandbox, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate" pentru o analiză în profunzime; - includă două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină; - includă modul de detectare, corelare si răspuns la evenimente de tip EDR („endpoint detection and response") capabil sa identifice amenințări avansate sau atacuri in curs de desfășurare; **<u>Cerințe minime a modulului de detectare, corelare și răspuns:</u>** **Acest modul trebuie să:**	pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. **<u>Protecție stații și servere fizice si virtualizate – caracteristici minime:</u>** Soluția antivirus: - 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 daca sunt infectate și blocarea procesului de criptare; - include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate); - include modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activitati suspecte în faza pre-executie; - include modul avansat de securitate pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fisierelor suspecte si 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 includere în sandbox, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate" pentru o analiză în profunzime; - include două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină; - include modul de detectare, corelare si răspuns la evenimente de tip EDR („endpoint detection and response") capabil sa identifice amenințări avansate sau atacuri in curs de desfășurare; **<u>Cerințe minime a modulului de detectare, corelare și răspuns:</u>** **Acest modul:**	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				- cuprindă - colectare de date si evenimente despre hardware si software aferent fiecărui endpoint, aducând informații detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox si modulul avansat de securitate – HyperDetect; - cuprindă componente ca senzori ce colectează și procesează datele respectiv partea de analiza de securitate care are ca obiect interpretarea acestora; - aibă capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și să poată raporta orice deviație de la acest comportament sub forma unui incident; - permită filtrarea incidentelor din interfața grafică în funcție de intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cît 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;	- cuprinde - colectare de date si evenimente despre hardware si software aferent fiecărui endpoint, aducând informații detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox si modulul avansat de securitate – HyperDetect; - cuprinde componente ca senzori ce colectează și procesează datele respectiv partea de analiza de securitate care are ca obiect interpretarea acestora; - are capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și să poată raporta orice deviație de la acest comportament sub forma unui incident; - permite filtrarea incidentelor din interfața grafică în funcție de intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cît și după IP, nume fișier, nume stație; - permite 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); - 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 poate genera/adaugă un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase;	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				- 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 unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare; - permită crearea regulilor de detecție customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; - permită creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea; - permită căutarea pro activă pe endpointurile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; - includă un modul de tip host IPS capabil sa blocheze atacuri la nivel de rețea incluzând mișcarea laterala a unor categorii de malware (modulul de tip host IPS să reprezinte o sursă de telemetrie / date despre atac pentru modulul de tip EDR, având abilitatea de a integra informații despre acțiunile luate de către o potențiala amenințare la nivel de rețea. **<u>Cerințe de sistem:</u>** - Sisteme de operare pentru stații de lucru: Windows 7/8.1/10 (inclusiv Embebed și IoT), Mac OS X 10.11. și mai recent, Red Hat Enterprise Linux / CentOS 6 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 14.04 și mai recent, SUSE Linux Enterprise Server 11 și mai recent, OpenSUSE 42 și mai recent, Fedora 25 și mai recent, Debian 8.0 și mai recent; - Sisteme de operare Windows pentru servere: Windows Server 2008/2008 R2/2012/2012 R2/2016/2019. **<u>Administrare și instalare remote:</u>** - Pachetele de instalare trebuie să fie configurabile cu modulele necesare: advanced threat control, anti-exploit, firewall,	- permite 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 unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare; - permite crearea regulilor de detecție customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; - permite creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea; - permite căutarea pro activă pe endpointurile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; - include un modul de tip host IPS capabil sa blocheze atacuri la nivel de rețea incluzând mișcarea laterala a unor categorii de malware (modulul de tip host IPS să reprezinte o sursă de telemetrie / date despre atac pentru modulul de tip EDR, având abilitatea de a integra informații despre acțiunile luate de către o potențiala amenințare la nivel de rețea. **<u>Cerințe de sistem:</u>** - Sisteme de operare pentru stații de lucru: Windows 7/8.1/10 (inclusiv Embebed și IoT), Mac OS X 10.11. și mai recent, Red Hat Enterprise Linux / CentOS 6 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 14.04 și mai recent, SUSE Linux Enterprise Server 11 și mai recent, OpenSUSE 42 și mai recent, Fedora 25 și mai recent, Debian 8.0 și mai recent; - Sisteme de operare Windows pentru servere: Windows Server 2008/2008 R2/2012/2012 R2/2016/2019. **<u>Administrare și instalare remote:</u>** - Pachetele de instalare sunt configurabile cu modulele necesare: advanced threat control, anti-exploit, firewall, network protection	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				network protection respectiv content control, device control, power user, patch management, full disk encryption, EDR sensor, exchange protection respectiv „relay" (cu sau fară „patch caching server"); - Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. **Consola de administrare trebuie să:** - includă secțiune, „Audit", unde se vor păstra toate acțiunile întreprinse de administratori și utilizatori ai consolei, cu informații detaliate: logare, editare, creare, delogare, permutare etc; - ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full - permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decît cele integrate în domen; - permită creare grupuri/subgrupuri, pentru endpointuri din retea dar care nu sunt integrate domen; - permită raportarea statiilor care sunt protejate respectiv neprotejate de catre solutie; - suporte definirea de portlet-uri (reprezentari grafice) configurabile. **Caracteristici și funcționalități principale ale modulului antivirus**: Produsul trebuie sa permită: - stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: 1. implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune; 2. alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină; 3. acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune; 4. acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină;	respectiv content control, device control, power user, patch management, full disk encryption, EDR sensor, exchange protection respectiv „relay" (cu sau fară „patch caching server"); - Există posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. **Consola de administrare:** - include secțiune, „Audit", unde se vor păstra toate acțiunile întreprinse de administratori și utilizatori ai consolei, cu informații detaliate: logare, editare, creare, delogare, permutare etc; - oferă posibilitatea de a crea pachetele de instalare de tip web installer sau kit full - permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decît cele integrate în domen; - permite creare grupuri/subgrupuri, pentru endpointuri din retea dar care nu sunt integrate domen; - permite raportarea statiilor care sunt protejate respectiv neprotejate de catre solutie; - suportă definirea de portlet-uri (reprezentari grafice) configurabile. **Caracteristici și funcționalități principale ale modulului antivirus**: Produsul permite: - stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: 1. implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune; 2. alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină; 3. acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune; 4. acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină;	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	*2*	*3*	*4*	*5*	*6*	*7*
				- scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la 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; - 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; - modul de antiphishing;	- scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la 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; - 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; - modul de antiphishing;	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	*2*	*3*	*4*	*5*	*6*	*7*
				- protecție în timp real pe mașinile cu sistem de operare Linux in 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 uni 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: 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 in mod curent in modul); d) Abilitatea de a acționa in mod diferit in funcție de tipul amenințării (fișier sau atac prin rețea); - posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este malițios; - oprirea atacurile 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. **Firewall:** - sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate;	- protecție în timp real pe mașinile cu sistem de operare Linux in 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 uni 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: 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 in mod curent in modul); d) Abilitatea de a acționa in mod diferit in funcție de tipul amenințării (fișier sau atac prin rețea); - posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este malițios; - oprirea atacurile 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. **Firewall:** - oferă posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate;	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				- modulul să poată fi instalat/dezinstalat la cerere; - să permită definirea de rețele de încredere pentru mașina destinație; **Protecția datelor:** - Produsul trebuie să permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **Controlul conținutului:** 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, violenta, pornografie etc). **Controlul aplicațiilor:** Pentru administrare și inventariere eficientă produsul trebuie să dețină un modul care va oferi posibilitatea de a: - efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe; - regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe; - bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subprocese) după: cale fișier: local, CD-ROM, portabil sau rețea, hash , certificat. **Controlul dispozitivelor:** Produsul trebuie să conțină un modul pentru controlul dispozitivelor care: - poate fi instalat/dezinstalat conform setărilor stabilite; - permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security	- modulul poate fi instalat/dezinstalat la cerere; - permite definirea de rețele de încredere pentru mașina destinație; **Protecția datelor:** - Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **Controlul conținutului:** 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, violenta, pornografie etc). **Controlul aplicațiilor:** Pentru administrare și inventariere eficientă produsul deține un modul care va oferi posibilitatea de a: - efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe; - regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe; - bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subprocese) după: cale fișier: local, CD-ROM, portabil sau rețea, hash , certificat. **Controlul dispozitivelor:** Produsul conține un modul pentru controlul dispozitivelor care: - poate fi instalat/dezinstalat conform setărilor stabilite; - permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				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; - 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. **Power User:** Produsul trebuie să conțină un modul pentru setări specifice – power user care să: - 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 suprascrie din consola setările aplicate de utilizatorii Power User. **Actualizare:** Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor: - 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. **Protecție și securitate pentru telefoane mobile de tip smartphone:** Produsul trebuie să ofere client de protecție pentru dispozitive mobile cu platforma Android (de la v. 2.2) și iOS (de la v 5.) Clientul mobil trebuie să: - permită asocierea unui dispozitiv cu un utilizator din Active Directory; - ofere posibilitatea instalării prin trimiterea unui email către utilizator cu detaliile de instalare;	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; - 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. **Power User:** Produsul conține un modul pentru setări specifice – power user care: - 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 suprascrie din consola setările aplicate de utilizatorii Power User. **Actualizare:** Produsul oferă posibilitatea de efectuare a actualizărilor: - 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. **Protecție și securitate pentru telefoane mobile de tip smartphone:** Produsul oferă client de protecție pentru dispozitive mobile cu platforma Android (de la v. 2.2) și iOS (de la v 5.) Clientul mobil: - permite asocierea unui dispozitiv cu un utilizator din Active Directory; - oferă posibilitatea instalării prin trimiterea unui email către utilizator cu detaliile de instalare;	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				- permită activarea dispozitivului mobil în consola de management prin scanarea unui cod QR; - asigure disponibilitatea pachetele de instalare pe Apple App Store si Google Play; - să poată întreprinde următoarele acțiuni: blocarea dispozitivului; deblocarea dispozitivului; ștergerea datelor si revenirea la setările din fabrica; localizarea dispozitivului; scanarea dispozitivului(doar pentru cele cu sistem de operare Android); criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android); - consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul sa aibă acces total asupra lui (rooted or jailbroken devices); - întreprindă automat acțiuni în cazul în care un dispozitiv nu este conform cu setările dorite: Ignorare; Blocarea accesului; Blocarea dispozitivului; Ștergerea datelor si revenirea la setările din fabrica; Ștergerea dispozitivului din consola; - ofere posibilitatea de a impune blocarea dispozitivelor cu ajutorul unei parole cu complexitate și perioada de expirare configurabilă, posibilitate de autoblocare a dispozitivului după un număr de minute definite de administrator; - ofere posibilitate de a genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet. precum: permiterea, blocarea sau programarea pentru anumite zile si intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet; - includă posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizarii browser-ului Safari; opțiunii de completare	- permite activarea dispozitivului mobil în consola de management prin scanarea unui cod QR; - asigură disponibilitatea pachetele de instalare pe Apple App Store si Google Play; - poate întreprinde următoarele acțiuni: blocarea dispozitivului; deblocarea dispozitivului; ștergerea datelor si revenirea la setările din fabrica; localizarea dispozitivului; scanarea dispozitivului(doar pentru cele cu sistem de operare Android); criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android); - consola permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul sa aibă acces total asupra lui (rooted or jailbroken devices); - întreprinde automat acțiuni în cazul în care un dispozitiv nu este conform cu setările dorite: Ignorare; Blocarea accesului; Blocarea dispozitivului; Ștergerea datelor si revenirea la setările din fabrica; Ștergerea dispozitivului din consola; - oferă posibilitatea de a impune blocarea dispozitivelor cu ajutorul unei parole cu complexitate și perioada de expirare configurabilă, posibilitate de autoblocare a dispozitivului după un număr de minute definite de administrator; - oferă posibilitate de a genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet. precum: permiterea, blocarea sau programarea pentru anumite zile si intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet; - include posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizarii browser-ului Safari; opțiunii de completare	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				automata a informațiilor; alertării utilizatorului în cazul accesării unor pagini frauduloase; Javascript; Pop-up-urilor; Cookie-uri. **Protecție și securitate pentru serverele de mail Microsoft Exchange (2019, 2016):** Soluția de protecție a serverelor de Exchange trebuie să: - ofere protecție antivirus, antispam (inclusiv antiphishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange cu posibilitatea de scanarea antivirus la cerere a bazelor de date Exchange; - asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail; - asigure actualizarea antivirus automat la un interval de maxim 1 ora, precum si la cerere; - includă, pe lîngă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor; - ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină); - ofere protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale; - ofere protecție antispam (cu o bază de semnături actualizabilă. Modulul antispam va trebui să includă un filtru URL cu o baza de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice; - ofere filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje;	automata a informațiilor; alertării utilizatorului în cazul accesării unor pagini frauduloase; Javascript; Pop-up-urilor; Cookie-uri. **Protecție și securitate pentru serverele de mail Microsoft Exchange (2019, 2016):** Soluția de protecție a serverelor de Exchange: - oferă protecție antivirus, antispam (inclusiv antiphishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange cu posibilitatea de scanarea antivirus la cerere a bazelor de date Exchange; - asigură scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail; - asigură actualizarea antivirus automat la un interval de maxim 1 ora, precum si la cerere; - include, pe lîngă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor; - oferă opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină); - oferă protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale; - oferă protecție antispam (cu o bază de semnături actualizabilă. Modulul antispam va trebui să includă un filtru URL cu o baza de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice; - oferă filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje;	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	*2*	*3*	*4*	*5*	*6*	*7*
				- ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute; - ofere posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori; - asigure actualizarea produsului va fi configurabilă și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu; - ofere statistici atît referitoare la scanarea antivirus cît și la scanarea antispam; - se integreze în cadrul consolei de management unitar al soluției antivirus în consola centrală unică. **Disk Encryption:** Soluție pentru managementul criptării discurilor pentru 353 calculatoare portabile. Soluția trebuie să acopere următoarele funcționalități minime: - Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus pentru mediul fizic (stații și servere), mediul virtual (VDI-uri si servere virtuale), căsuțe de email Exchange si dispozitive mobile (Android si iOS); - Clientul pentru disk encryption nu trebuie să fie ca un modul separat în cadrul clientului Antivirus; - produsul trebuie să folosească mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows si FileVault pentru Mac OSX; - Produsul trebuie să crypteze hard diskurile stațiilor de lucru integral; - Produsul trebuie să impună autentificarea utilizatorului înainte de startarea sistemei de operare (pre-boot authentication); - Produsul trebuie să păstreze cheile de criptare pe același server de management al protecției antivirus, managementul cheilor utilizate să fie efectuat din aceeași	- oferă un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute; - oferă posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori; - asigură actualizarea produsului va fi configurabilă și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu; - oferă statistici atît referitoare la scanarea antivirus cît și la scanarea antispam; - integrează în cadrul consolei de management unitar al soluției antivirus în consola centrală unică. **Disk Encryption:** Soluție pentru managementul criptării discurilor pentru 353 calculatoare portabile. Soluția acoperă următoarele funcționalități minime: - Administrarea produsului este realizată din aceeași consolă de management ca și soluția de protecție antivirus pentru mediul fizic (stații și servere), mediul virtual (VDI-uri si servere virtuale), căsuțe de email Exchange si dispozitive mobile (Android si iOS); - Clientul pentru disk encryption nu este un modul separat în cadrul clientului Antivirus; - produsul folosește mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows si FileVault pentru Mac OSX; - Produsul cryptează hard diskurile stațiilor de lucru integral; - Produsul impune autentificarea utilizatorului înainte de startarea sistemei de operare (pre-boot authentication); - Produsul păstrează cheile de criptare pe același server de management al protecției antivirus, managementul cheilor utilizate să fie efectuat din aceeași consolă comună,	

Denumirea bunurilor	Modelul articolului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	*2*	*3*	*4*	*5*	*6*	*7*
				consolă comună, inclusiv recuperarea rapidă a cheilor la solicitarea autorizată; - Produsul trebuie să ofere 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 trebuie să asigure criptarea pentru Următoarele OS: Windows 7 Enterprise (with TPM); Windows 8.1 Pro/ Enterprise; Windows 10 Pro/ Enterprise; WindowsServer 2008 R2 (withTPM); WindowsServer 2012/2012 R2, WindowsServer 2016, 2019, 2022, OSX 10.11/ 10.12. **Alte cerințe:** Perioada de suport și menținere de la producător: 1. Pentru soluția ofertată se solicită a fi 12 luni pentru perioada 12.01.2024-12.01.2025; 2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță. Notă: Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă (după caz).	inclusiv recuperarea rapidă a cheilor la solicitarea autorizată; - 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 7 Enterprise (with TPM); Windows 8.1 Pro/ Enterprise; Windows 10 Pro/ Enterprise; WindowsServer 2008 R2 (withTPM); WindowsServer 2012/2012 R2, WindowsServer 2016, 2019, 2022, OSX 10.11/ 10.12. **Alte cerințe:** Perioada de suport și menținere de la producător: 1. Soluția ofertată se va livra pentru 12 luni pentru perioada 12.01.2024-12.01.2025; 2. Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță. Notă: Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi executate de Ofertant, iar costul acestora sunt incluse în ofertă.	
TOTAL						

Semnat electronic: Digitally signed by Celonenco Vitalie
Date: 2023.11.21 21:47:00 EET
Reason: MoldSign Signature
Location: Moldova

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**