

Specificații tehnice

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1784732374102						
Obiectul achiziției: Pachete software antivirus						
Denumirea Serviciilor	Denumirea Serviciilor	Țara de origine	Producătorul	Specificația tehnică deplină solicitată de către entitatea contractantă	Specificația tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Pachete software antivirus (inclusiv Disk Encryption management)	Kaspersky Next EDR Optimum with 3 Year License	Elveția	Kaspersky	Conform anexei nr.1	Tip: Subscriere anuală pentru soluția de protecție și securitate pentru 1000 entități (PC/ laptop/ VDI/ Server) pentru perioada de 3 ani. Ofertantului este responsabil de a determina modelul de licențiere luând în calcul: 1000 entități (PC/laptop/VDI/Server); Disk Encryption management pentru 1000 entități. Produsul antivirus 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, gândită 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; Serviciu de corelare și răspuns la evenimente de tip EDR (endpoint detection and response). Consola de management: Accesibilitate atât de pe browser desktop cât și tip mobile. Oferă opțiuni configurabilă de actualizare automată a consolei de management. Soluția de scanare centralizată: Soluția asigură protecția mediilor virtualizate (VDI), inclusiv a mediilor persistente și non-persistente, și este compatibilă cu următoarele platforme de virtualizare: 1. VMware vSphere;	ISO 9001:2015 Calitate, ISO 14001:2015 Mediu, ISO 37001:2016 Anti-mita, ISO 20000-1:2018 Servicii IT ISO 27001:2013 Securitatea Informației ISO 22301:2019 Continuitatea Afacerii

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

				2. Citrix XenServer; 3. Microsoft Hyper-V. Cerințe generale produs: Soluția: 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, alertează administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile. Panou de monitorizare și raportare (Dashboard): 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). Inventarierea rețelei – managementul securității: Produsul: se integrează cu domenii Active Directory multiple, să poată 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; 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.	
--	--	--	--	--	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

					Politici: 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: permite setarea de opțiuni specifice pentru afișarea rapoartelor existente; deține un panou central care afișează statutul modulelor și rapoartele lor pentru perioadele de timp specificate; conține rapoarte care prezinta statutul 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 oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, include 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); Carantină: Produsul permite restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă; Administrarea Carantinei este posibilă atât pe terminalul administrat	
--	--	--	--	--	--	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

					cât și din consola de management; Utilizatori: Administrarea va fi 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 vor putea fi importați din Microsoft Active Directory sau creați în consola de management; Va fi posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil. Log-uri: Soluția va permite înregistrarea acțiunilor utilizatorilor și va oferi informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. Actualizare: Soluția va permite: 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. Protecție stații și servere fizice și virtualizate: 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 risc capabil să identifice și să remedieze riscurile identificate la nivel de rețea sau sistem de operare, cu posibilitate de configurare și automatizare; Include un modul avansat de securitate bazat pe tehnologii de machine learning, analiză comportamentală și algoritmi euristici, proiectat pentru detectarea atacurilor avansate și a activităților suspecte înainte de faza de 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 trebuie să i se poată configura independent nivelul de protecție și acțiunile aplicate, în funcție de capacitățile	
--	--	--	--	--	---	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

					soluției oferite și recomandările producătorului; Include modul de sandbox, unde se vor putea 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, tipurile de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. 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 ; 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 cît și după IP, nume fișier, nume stație; Permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: 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 poate genera/adauga 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 a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permite 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;	
--	--	--	--	--	---	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

				Permite crearea regulilor de detecție customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; Permite crearea regulilor de excludere customizabilă 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 privilegii 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: 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) ofere senzori de colectare a datelor și componente de procesare și interpretare a acestora; c) posedă capacitarăți de evaluare a activității tipice a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining”) și va raporta orice deviație de la acest comportament sub forma unui incident; d) ofere 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); 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; f) poate exclude fișiere non-malițioase de la acțiunea de investigare sau poate genera/adauga un set de fișiere malițioase într-o listă pentru a	
--	--	--	--	--	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

					preveni mișcarea laterală a fișierelor/proceselor malițioase; g) permită vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri. Cerințe de sistem: Sisteme de operare pentru stații de lucru: Windows 7/10/11 (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. Administrare și instalare remote: 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 sunt 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 instale/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. Caracteristici și funcționalități principale ale modulului antivirus: Produsul va permite: Stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: 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 scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau	
--	--	--	--	--	--	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

					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 viruși 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 oferi protecție anti-spyware; Setarea priorităților scanărilor programate; Soluția va permite configurarea mecanismelor de scanare utilizând tehnologii locale, bazate pe cloud sau alte mecanisme echivalente oferite de producător, pentru optimizarea performanței și consumului de resurse; Administratorul va putea configura politicile și mecanismele de scanare disponibile, inclusiv utilizarea tehnologiilor locale, bazate pe cloud sau a altor mecanisme echivalente, în funcție de infrastructura protejată și recomandările producătorului; 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 dezințalare; Modul de antiphishing; Protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată; Soluția va suporta implementarea în medii VDI persistente și non-persistente, inclusiv utilizarea imaginilor de referință (Golden Image/Template) sau a unor mecanisme echivalente oferite de producător; 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 configura acțiunile aplicate amenințărilor detectate, inclusiv raportarea, monitorizarea sau blocarea acestora;	
--	--	--	--	--	---	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

				c) abilitatea de a configura nivelul de sensibilitate al mecanismelor de detecție și politicilor de securitate, conform recomandărilor producătorului; 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. Firewall: Oferă posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; Modulul va putea fi instalat/ activat/ dezactivat/ dezinstalat la cerere; Permite definirea de rețele de încredere pentru mașina destinație. Protecția datelor: conform clarificarilor a fost exclus Controlul conținutului: Produsul va oferi 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 dispozitivelor: Produsul va 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 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	
--	--	--	--	--	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

					pentru care s-au configurat reguli. Power User: Produsul va 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 suprascrise din consola setările aplicate de utilizatorii Power User. Actualizare: Produsul va oferi 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. Gestionabil – doar local sau și servere online. Protecție Anti-Tampering: 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 compatibilă cu sistemele de operare Windows și Linux; 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. Disk Encryption: Soluție pentru managementul criptării discurilor pentru 1000 entități. Soluția va oferi următoarele funcționalități: Administrarea produsului va fi 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;	
--	--	--	--	--	--	--

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md

					Produsul va asigura criptarea pentru Următoarele OS: Windows 7/10/11 Pro/Enterprise (with TPM); WindowsServer 2012/2012 R2, 2016, 2019, 2022 (with TPM), OSX de la 10.12. Perioada de suport și mentinere de la producător: 1. Pentru soluția oferată - 36 luni; 2. Producătorul va oferi suport 24/24, prin e-mail sau conectare de la distanță. Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi executate de Ofertant, iar costul acestora sunt incluse în ofertă.	
--	--	--	--	--	---	--

- Acest tabel este completat de către ofertant în coloanele 2, 3, 4, 6, 7.

Numele, prenumele: Bogdan GNIDAS

(Se precizează numele și prenumele persoanei ce aplică semnătura)

În calitate de: Administrator

(Se precizează funcția în cadrul companiei)

Ofertantul: BTS Pro SRL

(Se precizează denumirea operatorului economic)

Adresa: Mun. Chișinău, str. Ion Creangă, 6 V

(Se precizează adresa juridică a operatorului economic)

(Semnătura)

L.Ș.

str. Ion Creangă 6V
MD-2069, Chișinău, Republica Moldova
Tel.: +373 22 870 140
Fax.: +373 22 595 858

Cod TVA: 0505766
Cod BIC: MOLDM2X336
Cod fiscal: 1008600061565
Cod IBAN: MD22ML000000022515361542

"BTS Pro" SRL
office@bts.md
www.bts.md