Specificaţii tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloanele 3, 4, 5, 7, iar de către autoritatea contractantă – în coloanele 1, 2, 6, 8]

Numărul procedurii de achiziţie - conform SIA RSAP din din ocds-b3wdp1-MD-1595939704756 din 28.07.2020

Denumirea procedurii de achiziţie: **Soluţie corporativă antivirus de protecţie şi securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate.**

Cod CPV	Denumirea bunurilor solicitate	Modelul articolu-lui	Ţara de origine	Produ-cătorul	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	8
48700000-5	Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate.	Bitdefender	România	România	I. **Cerintele tehnice functionale minim solicitate:** -Solutie corporativa antivirus de protectie si securitate in varianta Cloud, pentru o perioada de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate. -Solutia trebuie sa asigure protectie si management centralizat pentru statii de lucru, servere si dispozitive mobile cu urmatoarele sisteme de operare: Statii de lucru: -Microsoft Windows 7 Service Pack 1; 8.1; 10; (all 32-bit and 64-bit editions); -macOS 10.12, 10.13, 10.14; Servere: -Microsoft® Windows Server 2008 R2; 2012; 2012 Essentials; 2012 R2; 2012 R2 Essentials; 2012 R2 Foundation; 2016 Standard; 2016 Essentials; 2016 Datacenter: 2016 Core; 2019 Standard; 2019 Essentials; 2019 Datacenter; 2019 Core; CentOS, Debian, Oracle Linux, RHCK and UEK, RHEL, SUSE Linux Enterprise Server 11 SP3, SP4, Ubuntu, etc. Dispozitive Mobile: -Android 4.03 and later; iOS 9.x and later -Solutia ofertata trebuie sa fie una bazata pe tehnologia Cloud, care sa ofere un management centralizat a tuturor dispozitivelor: statii de lucru, servere si dispozitive mobile; -Solutia trebuie sa asigure protectie in timp real, impotriva virusilor (ransomware - crypto) cu scopul prevenirii distrugerii si modificarii datelor, amenintarilor spyware, rootkit-urilor, tentativelor de intruziune, spam-urilor si a altor mesaje nedorite.	Conform Cerințelor tehnice a Autorității contractante. Matrice de corespundere Servicii Instalare, configurare, punere in functiune a solutiei	ISO 9001 ISO 27001

Digitally signed by Cioclea Victor
Date: 2020.08.02 22:20:23 EEST
Reason: MoldSign Signature
Location: Moldova

					-Solutia trebuie sa ofere actualizari automate a versiunilor noi si a hotfix-urilor; -Solutia trebuie sa ofere protectie impotriva virusilor si noilor amenintari necunoscute care sa fie bazata pe analize euristice, de comportament si reputatie; -Solutia trebuie sa includa patch management cu optiuni pentru excluderi si actualizari manuale si analiza vulnerabilitatilor din retea; -Solutia trebuie sa ofere functionalitati de firewall, intrusion prevention application control si sanbox pentru analiza traficului de tip ransomware si detonarea acestuia; -Solutia trebuie sa asigure criptarea automata prin VPN, a intregului traffic realizat dintre dispozitivele mobile, permitand utilizarea in conditii de siguranta a Wi-Fi public si retelelor mobile; -Solutia trebuie sa ofere posibilitati exacte de activare si dezactivare de configurare a funcfionalitatilor precum: scanarea antivirus la cerere, firewall gestionat, controlul accesului la Internet, controlul aplicatiilor care sa blocheze executarea aplicatiilor si scripturilor conform regulilor create sau definite de administrator, scanarea traficului web, controlul dispozitivelor; -Solutia trebuie sa ofere posibilitatea de aplicare a politicilor pe masini, client, grupuri de masini, domeniu, unitati organizationale sau utilizatori de AD; -Solutia trebuie sa ofere instalare centralizata a statiilor de lucru si terminalelor mobile; -Solutia trebuie sa ofere consola unica de management cu instalare in cloud; -Solutia trebuie sa ofere functional Multi-engine anti-malware; -Solutia trebuie sa includa functionalul de Patch Management, pentru a asigura actualizarea de software atit de la produsele Microsoft,cit si pentru alte aplicati de la terti; -Solutia trebuie sa ofere functional de Firewall ce va permite setarea unor reguli bazate pe actiuni (blocarea sau permiterea) si directie (intrare sau iesire) pentru controlul si monitorizarea traficului la nivel de endpointsi retea, care sa furnizeze un nivel de securitate suplimentar, aflat deasupra regulilor utilizatorului pentru Windows Firewall si a altor reguli pentru domenii. -Solutia trebuie sa ofere functional de Protectie Web: protejarea accesarilor pe site-uri bancare (Control conexiune) care sa alerteze utilizatorii atunci cand astea au o conexiune securizata catre site-uri si de operatiuni bancare online si catre alte site-uri precizate care		

					trateaza informatii sensibile; blocarea site-urilor cunoscute ca fiind daunataore (Navigare bazata pe reputatie); impiedicarea accesului la site nepermise (Controlul continutului Web); blocarea accesului la tipurile de continut nepermise (Filtrare tipuri de continut). -Solutia trebuie sa ofere functional de Controlul conexiunilor prin securizarea platilor online si afisarea unui pop-up care blocheaza celelalte pagini si imposibilitate accesarii altor decat cea in care se efectueaza tranzactia. -Solutia trebuie sa ofere functional de scanare in timp real a tuturor obiectelor pe care le acceseaza utilizatorii finali, pentru depistarea programelor de tip malware si inclusiv sa ofere posibilitatea de configurare si efectuare a scanarii manuale; -Solutia trebuie sa ofere functional de scanare a aplicatiilor in cloud -Solutia trebuie sa ofere functional de Scanare a semnaturilor; -Solutia trebuie sa includa functional de control a dispozitivelor externe, sa ofere posibilitatea: de a seta restrictii in privinta modului in care utilizatorii pot accesa dispozitive USB, precum dispozitive de stocare, camere USB si imprimante; de a interzcie accesul la orice dispozitiv de stocare USB; de a stopa rularea executabilelor stocate pe astfel de dispozitive; de a seta restrictii pe grupuri de dispozitive; -Solutia trebuie sa ofere functional de analiza euristica si zero day, de comportament si reputatie; -Solutia trebuie sa ofere functional de Sandbox automatizat inclus - pentru analiza amanuntita prin detonarea fisierilor malitioase sau care nu pot fi protejate in baza de semnatura sau comportament; -Solutia trebuie sa ofere functional de control al aplicatiilor, prin setarea unor reguli de blocare create ca excluderi pentru a bloca un acces anume si sa fie bazate: •pe actiuni precum permiterea, blocarea, sau permiterea si monitorizarea aplicatiilor; •pe evenimente precum pomire aplicatie, incarcare modul, pomire program de instalare, acces la fisiere, pomire aplicatie si incarcare modul; •prin stabilirea unor conditii care sa poata fi selectate dupa atribute (cale destinatie, nume filler destinatie, reputatie destinatie, versiune fisier destinatie, cod hash pentru certificat la destinatie, etc), conditie si valoare, ce vor asigura activarea regulilor de excludere; -Solutia trebuie sa ofere functional de Management API prin integrarea solutiilor terte precum: SIEM/RMM; **II. Cerintele tehnice vis-a-vis de administrarea solutiei:**		

					-Administrarea solutiei ofertate este necesara sa se faca printr-o singura consola de administrate bazata pe cloud, fara ca sa necesite careva echipamente hardware(servere de management) sau careva software special, -Consola de administrate trebuie sa fie capabila de a functiona pe orice dispozitiv si sa contina toate funtionalitatile sus solicitate; -Sa suporte urmatoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; -Interfata consolei de administare trebuie sa asigure posibititatea de functionare in limbile: romana, rusa si engleza obligatoriu, cu capacitatea de a putea fi selectata limba dorita, in scopul unei administrari mai usoare de catre administratori; -Administratorul trebuie sa poata permite sau interzice utilizatorului de a activa sau dezactiva caracteristicile de securitate setate; **III. Cerinte vis-a-vis de functionalul de raportare si alerte:** -Solutia trebuie sa permita generarea de rapoarte grafice detaliate, saptaminal sau lunar, cu posibilitate de export minimum in format (csv), inclusiv cu remitere automata catre adrese de email specificate, rapoartele trebuie sa cuprinda minim informatie despre: •Clasament computere (dupa infectii blocate); •Top de infectii tratate; •Infectii gestionate; •Starea de protectie; •Cele mai recente actualizari pentru definitiile de malware pe computere; •Daca s-au instalat actualizarile de securitate; -Solutia trebuie sa permita setarea si configurarea de alerte, declansarea lor sa poata fi aplicata pentru minim urmatoarele actiuni: blocat, redenumit, oprit, sters, plasat, raportat, dezinfectat, in carantina, raportat catre utilizator, blocat si actiune suplimentara solicitata de la utilizator, mutat in cosul de gunoi; -Solutia trebuie sa asigure posibilitatea de trimitere a alertelor in momentul declansarii prin email specificat de administrator si sa permita setarea limbii dorite in care sa fie emailul (minim romana, engleza, rusa); **IV. Alte cerinte obligatorii:** -Pentru solutia ofertata se solicita a fi 12 luni suport local si de la producator. -Producatorul trebuie sa ofere suport 24/24, prin e-mail sau conectare de la distanta, inclusiv suport local din partea partenerului.		

					-Lucrarile de instalare, configurare, punerea in functiune a solutiei trebuie sa fie executate de ofertant, iar costul acestora trebuie sa fie incluse in oferta comerciala. -Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securitatii informationale conform ISO 27001:2013; -Solutia trebuie sa se regaseasca in Gartner in ultimii 3 ani de zile si sa ocupe locuri de top in testele Internationale “AV-TEST”.		
Total							

Semnat:_____

Numele, Prenumele: Victor Cioclea

În calitate de: Administrator

Ofertantul: S.C. „RTS ONE” S.R.L.

Adresa: mun. Chișinău, str. Mit. Bănulescu-Bodoni 59/B of. 815