Тендерлік құжаттамаға
6-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы	"КАЖсервис" жауапкершілігі шектеулі серіктестігі
Ұйымдастырушының атауы	"КАЖсервис" жауапкершілігі шектеулі серіктестігі
Тендердің №	№ 17631241-1
Тендердің атауы	Желілік қауіпсіздік құрылғысын сатып алу (желілік экран)
Лоттың №	№ 87788114-ОТ1
Лоттың атауы	Арнайы экран
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*	263021.900.000009
Тауардың атауы*	Арнайы экран
Өлшем бірлігі*	Дана
Саны (көлемі)*	1
Бірлік бағасы, қосылған құн салығын қоспағанда*	4740000
Қосылған құн салығын қоспағанда, сатып алуға бөлінген жалпы сома*	4740000
Жеткізу шарты (ИНКОТЕРМС 2010-ға сәйкес)*	DDP термині келу орнын көрсете отырып қолданылады. Бұл сатып алушының елінде көрсетілген жерге тауар жеткізілгеннен кейін сатушының жауапкершілігі аяқталатынын білдіреді. Жүктерді жеткізу бойынша барлық тәуекелдер, барлық шығыстар (салықтар, баждар және т.б.), импорт кезінде төленетін баждар мен басқа да төлемдерді қоса алғанда, тауардың бүлінуі мен жоғалуы үшін жауапкершілік осы уақытқа дейін сатушыға жүктеледі, сатушы сонымен қатар кедендік тазартуға жауап береді
Жеткізу мерзімі*	В течении 16 календарных дней после получения заявки от Заказчика
Аванстық төлем мөлшері*	0
Ұлттық стандарттардың атауы, ал олар болмаған жағдайда сатып алынатын тауарларға арналған мемлекетаралық стандарттар. Ұлттық және мемлекетаралық стандарттар болмаған кезде мемлекеттік сатып алуды нормалауды ескере отырып, сатып алынатын тауарлардың талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары көрсетіледі.	
Шығарылған жылы (Тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс)	2026
Кепілдік мерзімі (айлармен)	12

Сатып алынатын тауарлардың қажетті функционалдық, техникалық, сапалық, өнімділігі мен басқа да сипаттамаларының сипатталуы	Жалпы талаптар Келесі буын желіаралық экраны – 1 дана. Жабдық жаңа, қапталған және бұрын пайдаланылмаған болуы тиіс. Бұрын пайдаланылған, қалпына келтірілген, қайта өңделген немесе қандай да бір тәсілмен түрлендірілген жабдыққа жол берілмейді. Қаптамадағы өндірістік код жабдықтың өзіндегі өндірістік кодпен сәйкес келуі тиіс. Қатысуға арналған өтінім құрамында парт-нөмірлері мен сипаттамасы көрсетілген егжей-тегжейлі техникалық ерекшелік қоса берілуі тиіс. Желіаралық экранның техникалық сипаттамалары Келесі буын желіаралық экранына қойылатын талаптар. Қауіпсіздік шлюзі желі ағындарын бақылау және басқару үшін трафик пен қолданбалардың күйін егжей-тегжейлі талдауға негізделген күйді бақылауды пайдалануы керек. Шешім сервер және ретранслятор (relay) режимдерінде DHCP қолдауы керек. Шешім Transparent (Bridge) режимінде жұмыс істеу мүмкіндігін қолдауы керек. Шешім OSI үлгісінің екінші деңгейінде жұмысты қамтамасыз етуі керек (көпір режимі). Көпір режимінде шешім келесі мүмкіндіктерді қолдауы керек: желіаралық экран; Басып кірудің алдын алу және анықтау жүйесі (IPS/IDS); URL сүзгісі; Ботнет белсенділігінен қорғау (Антибот); Вирусқа қарсы қорғаныс (Антивирус); Қолданбаны басқару; Шифрланған трафикті тексеру (HTTPS инспекциясы); Пайдаланушыны сәйкестендіру және басқару құралдары (Identity Awareness); Күдікті нысандарды талдауға және оқшаулауға арналған оқшауланған орта механизмі (Sandboxing). Шешім көпір режимінде белсенді/күту режиміндегі кластерлеуді қолдауы керек. Шешім желілік қосылым күйлерін синхрондау арқылы шлюздің жоғары қолжетімділігін қолдауы керек. Шешім IPv6 протоколын қолдауы керек. Шешім QoS механизмдеріне негізделген саясаттарды қолдауы керек. Шешім белгілі бір көз IP, тағайындалған IP немесе қызмет үшін өткізу қабілетіне кепілдік беру немесе шектеу және кіріс уақытын басқару мүмкіндігін қамтамасыз етуі керек. Шешім өткізу қабілеттілігіне басымдық беру, шектеу немесе кепілдік беру үшін параметрлерді икемді анықтау мүмкіндігін қоса, VPN трафигі үшін QoS ережелерінің конфигурациясын қолдауы керек. Шешім Басып кірудің алдын алу жүйесінің (IPS) функционалдығын қамтамасыз етуі керек. IPS жүйесі келесі механизмдерге негізделген қауіпті анықтауды қамтамасыз етуі керек: Белгілі шабуылдар мен эксплуаттарды анықтау үшін сигнатуралық талдау; әдеттен тыс немесе зиянды трафикті анықтау үшін протокол аномалиясын бақылау және талдау; Қажетсіз қолданба әрекетін бақылау және блоктау үшін қолданбаларды басқару; Бұрын белгісіз шабуылдар мен аномальды мінез-құлықты анықтау үшін мінез-құлыққа негізделген анықтау. Шешім веб-қосымшаларды зиянды кодтар мен шабуылдардан қорғау үшін кіріктірілген енуді болдырмау жүйесінің (IPS) функционалдығын қамтамасыз етуі керек. Жүйе құрттарды, буфер толып кету шабуылдарын, SQL инъекциясын, пәрменді енгізуді, сайттар аралық сценарийлерді (XSS) блоктауы және реттелетін HTTP құрт блокаторын қолдауы керек. Сонымен қатар, жүйе каталогтарды өтуден, зиянды немесе қате HTTP тақырыптарынан (Header Rejection), сондай-ақ зиянды HTTP кодынан қорғауды қамтамасыз етуі керек. Шешім пайдаланушы сәйкестендіру және басқару функцияларын қамтамасыз етуі керек. Microsoft Active Directory қауіпсіздік оқиғаларын талдау арқылы пайдаланушы сәйкестіктерін алу мүмкіндігі болуы керек. Домендік емес құрылғылар мен пайдаланушылар үшін браузер негізіндегі пайдаланушы идентификаторының аутентификациясын қолдауы керек. пайдаланушылардың компьютерлерінде саясат бойынша орнатылатын және идентификаторларды жинап, қауіпсіздік шлюзіне жібере алатын арнайы агент болуы керек. Шешім қолданбаларды басқару және URL-сүзгілеу функцияларын қамтамасыз етуі керек. Қолданбаларды басқару дерекқорында 10000-нан астам белгілі қолданбалар болуы керек. Шешім кем дегенде 255000 Web 2.0 виджеттері үшін қауіпсіздікті егжей-тегжейлі бақылауды қамтамасыз етуі керек. Шешім 200 миллионнан астам URL мекенжайларының URL санаттарын қамтамасыз етуі керек. Шешім ботнет белсенділігінен және антивирустық қорғаудан (Anti-Bot және Antivirus) қорғауды қамтамасыз етуі керек. Anti-Bot қолданбасы ықтимал ботнет инфекциясын көрсететін аномальды желі әрекетін анықтай алуы және мұндай әрекеттің автоматты түрде тоқтатылуын қамтамасыз етуі керек. Anti-Bot қолданбасы IP репутациясын, URL және DNS мекенжайларын және байланыс протоколының үлгілеріне негізделген ботты анықтауды қамтитын көп деңгейлі анықтау механизмін пайдалануы керек, сонымен қатар DGA-дан қорғау механизмдерін қоса, DNS протоколының шабуылдарынан автоматты түрде қорғау үшін интеллектуалды талдауды қолданатын механизмдерге ие болуы керек. Вирусқа қарсы қолданба зиянды веб-сайттарға кіруге жол бермеуі және кіріс зиянды файлдарды анықтауы және блоктауы керек. Вирусқа қарсы қолданба SSL шифрланған трафикті сканерлей алуы керек. Шешім SSL трафикті тексеру функциясын қамтамасыз етуі керек. Шешім лицензияға сәйкес Sandboxing функциясын (бұлтта немесе арнайы жергілікті құрылғыда тексеру) қамтамасыз етуі керек. Оқшауланған орта (Sandboxing) функциясы нөлдік күндік шабуылдардан, сондай-ақ бұрын белгісіз зиянды бағдарламалық құралдан қорғауды қамтамасыз етуі керек. Жүйе сәйкес статикалық қолтаңбалар шығарылғанға және таратылғанға дейін мұндай қауіптердің алдын алуды қамтамасыз етуі керек. Оқшауланған ортаны енгізу топологиясы: Желілік оқшауланған орта режимін қолдау (желі негізінде); Трафик тұрғысынан жұмыс режимін қолдау - Inline (Көпір режимі); Пошта тасымалдау агенті режимін қолдау; Айналанған трафикті талдау режимін қолдайды (TAP/SPAN порты). Шешім электрондық пошта мен веб-трафикті қорғауға арналған бөлек инфрақұрылымды қамтымауы керек. Шешім ақауларға төзімділікті қамтамасыз ету үшін кластерлеуді қолдауы керек. Шешім әртүрлі файл түрлерін, соның ішінде орындалатын файлдарды, мұрағаттарды және құжаттарды эмуляциялау функционалдығын қолдауы керек, сонымен қатар Java және Flash эмуляциясын қолдауы керек. Эмуляция механизмі әртүрлі операциялық жүйелерді, соның ішінде Windows XP, 7, 8.1, 10 және 11-ді қолдауы керек, сондай-ақ арнайы конфигурацияланған кескіндерді (Customized images) пайдалану мүмкіндігін қамтамасыз етуі керек. Эмуляция механизмі зиянды әрекетті тексеру, эмуляциялау және алдын алу функцияларын қамтамасыз етуі керек, сонымен қатар зиянды бағдарламаға қарсы инфрақұрылымға оқиғалар туралы есеп беруді қамтамасыз етуі керек. Шешім шағын өлшемді және 100 МБ дейінгі өлшемдегі файлдардың эмуляциясын қамтамасыз етуі керек. Шешім осалдықтарды пайдалану (exploitation) кезеңіндегі шабуылдарды анықтап, shell code іске қосылуына жол бермеуі және зиянды бағдарламалық кодты жүктеу немесе орындау мүмкіндігін болдырмауы керек. Шешім орталық процессор нұсқауларының орындалу ретін бақылау арқылы ROP (Return Oriented Programming) және осалдықтарды пайдаланудың басқа әдістерін, соның ішінде артықшылықтарды арттыруды (Privilege Exploitation) анықтауды қамтамасыз етуі керек. Шешім нөлдік күндік шабуылдардан және белгісіз зиянды бағдарламалардан қорғау үшін электрондық пошта хабарларының ішіндегі сілтемелерді сканерлей алуы керек. Шешім зиянды кодтан оқшауланған ортаны анықтау әрекеттеріне қарсы тұруды қамтамасыз етуі және оқшауланған ортаның орындалуын анықтау әдістерімен күресуге арналған құралдарды қамтуы керек. Шешім орталықтандырылған басқару жүйесімен интеграцияланууы және басқаруды, қауіпсіздік саясатын конфигурациялауды және бір нүктеден бақылауды қамтамасыз етуі керек. Шешім әрбір вирус жұққан файлды талдау нәтижелеріне негізделген егжей-тегжейлі есепті құруы керек. Шешім ықтимал қауіпті деп жіктелген құжаттың қауіпсіз көшірмесін лезде жеткізу механизмін қолдауы керек, бұл ретте түпнұсқа құжат әрі қарай талдау мен тексеруге жатады. Шешім ықтимал қауіптерден келесі құжаттарды тазалау технологияларын қолдауы керек: Түпнұсқа пішімдеуді, сілтемелерді бейтараптандыруды және мәтінді таңдау және көшіру мүмкіндігін сақтай отырып, PDF форматына түрлендіру; Бастапқы пішімді сақтау және белсенді мазмұнды жою кезінде түрлендіру: сценарийлер, макростар, белсенді сілтемелер, кірістірілген нысандар, стандартты емес және стандартты өрістер. Шешім пайдаланушыларға оқшауланған ортада тексерілгеннен кейін бастапқы файлдарды сұрауы үшін өзіне-өзі қызмет көрсету веб-порталын қолдауы керек. Шешім бастапқы файл пішімін қолдау және жойылуы тиіс мазмұн түрлерін көрсету үшін икемді параметрлерді қамтамасыз етуі керек. Шешім веб-ресурстарға қол жеткізген кезде белгісіз зиянды бағдарламалық құралды (пациент-0) нақты уақытта блоктауды қамтамасыз етуі керек. Шешім электрондық пошта арқылы таратылатын белгісіз зиянды бағдарламалық құралды (пациент-нөл) нақты уақытта блоктауды қамтамасыз етуі керек. Шешім IPSec VPN функциясын қамтамасыз етуі керек. Шешім кірістірілген сертификат орталығын (CA) және сыртқы үшінші тарап сертификаттау орталықтарын пайдалануды қолдауы керек. Шешім IKEv2 (I және II фазалар) үшін 3DES және AES-256 шифрлауын, сондай-ақ II кезең үшін Suite-B-GCM-128 және Suite-B-GCM-256 алгоритмдерін қолдауы керек. Шешім кем дегенде келесі Diffie-Hellman топтарын қолдауы керек: 1-топ (768 бит), 2-топ (1024 бит), 5-топ (1536 бит), 14-топ (2048 бит), 19-топ және 20-топ. Шешім алгоритмдерді пайдалана отырып, кем дегенде келесі деректер тұтастығы механизмдерін қолдауы керек: MD5, SHA-1 SHA-256, SHA-512 және AES-XCBC. Шешім келесі желі топологияларында Site-to-Site VPN қосылымдарын жүзеге асыруды қолдауы керек: Толық байланысқан желі (барлығы-барлығымен); Жұлдызды желі (орталық сайтқа қашықтағы кеңселер); Тармақталған желі (орталық сайт арқылы басқа қашықтағы сайтқа қашықтағы торап). Шешім қашықтан мобильді қатынасты қамтамасыз етуі керек Шешім кемінде 200 бір уақытта пайдалануы қосылымдары үшін қашықтан мобильді қатынас мүмкіндігін қамтамасыз етуі керек. Шешім екі факторлы аутентификацияны сыртқы екі факторлы аутентификация жүйелерімен біріктіру арқылы да, өндірушісі ұсынған кірістірілген екі факторлы аутентификация механизмі арқылы да қамтамасыз етуі керек. Шешім келесі мүмкіндіктерді қамтамасыз етуі керек: VPN арқылы пайдаланушыға қауіпсіз қол жеткізу; Қол жеткізуді басқару үшін мобильді құрылғыларды нақты соңғы пайдаланушыларға сәйкестендіру және байланыстыру; Қосылған соңғы нүктелердің корпоративтік қауіпсіздік саясатының талаптарына сәйкес келетініне сәйкестігін қамтамасыз етуі керек. Шешімде кірістірілген SD-WAN функциясы болуы керек. Шешім IoT құрылғыларын қорғауға арналған арнайы қызметтердің функционалдығын қамтамасыз етуі керек (қосымша лицензия болған жағдайда). Шлюзге қойылатын техникалық талаптар Өнімді желі интерфейстері (ең төменгі талаптар): 8 x 1 Гбит/с LAN RJ-45 порты; 1 x 1 Гбит/с WAN RJ-45 порты; 1 x 1 Гбит/с DMZ SFP порты; 2 x 10 Гбит/с LAN/WAN SFP+ порты; 1 қуат қосқышы. 1 x USB 3.0 Type-A. 1 USB Type-C консоль порты. 2 x қуат көзінің қосқышы. Желіаралық экранның өткізу қабілеті: кемінде 8990 Мбит/с. IPS өткізу қабілеті: кемінде 6890 Мбит/с. NGFW өткізу қабілеті (желіаралық экран, қолданбаларды басқару және IPS функциясы белсендірілген): кемінде 4990 Мбит/с. Қауіптердің алдын алу өткізу қабілеті (желіаралық экран, қолданбаларды басқару, URL сүзгілеу, IPS, антивирус, анти-бот және бұлттық оқшауланған орта функциясы қосылған): кемінде 2490 Мбит/с. Желіаралық экран 1518B UDP кемінде 15490 Мбит/с. Желіаралық экранның кешігуі (орташа) 24 µSec. VPN AES-GCM 1452B өткізу қабілеті: кемінде 4490 Мбит/с. Жаңа қосылымдар: кемінде 62000 қосылым/с. Бір мезгілде қосылымдар: кемінде 2 миллион. Қолдау және жазылу. Өндірушіден 3 жылға техникалық қолдау, 7 x 24, жабдықты кепілдікпен ауыстыру. Өндірушіден 3 жыл мерзімге жазылу, қауіпсіздік сервистеріне барлық қажетті жазылымдар қамтылуы тиіс.
Ілеспе қызметтер (қажет болған жағдайда көрсетіледі) (монтаждау, іске қосу, дайындау, тексеру және тауарларды сынау)	

Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді)	

* мәліметтер сатып алу жоспарынан алынады (автоматты түрде көрсетіледі).

Ескерту:

1. Функционалдық, техникалық, сапалық, пайдаланушылық, өзге де сипаттамалар, ілеспе қызметтер бойынша әрбір талап және қосымша талаптар бөлек жолда көрсетіледі.

2. Өзге құжаттарда техникалық ерекшеліктің талаптарын белгілеуге жол берілмейді.

Приложение 6
к тендерной документации

Техническая спецификация закупаемых товаров (заполняется заказчиком)

Наименование заказчика	Товарищество с ограниченной ответственностью "КАЖсервис"
Наименование организатора	Товарищество с ограниченной ответственностью "КАЖсервис"
№ тендера	№ 17631241-1
Наименование тендера	Закупки сетевого устройства безопасности (межсетевой экран)
Номер лота	№ 87788114-ОТ1
Наименование лота	Экран специальный
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*	263021.900.000009
Наименование товара*	Экран специальный
Единица измерения*	Штука
Количество (объем)*	1
Цена за единицу, без учета налога на добавленную стоимость*	4740000
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*	4740000
Условия поставки (в соответствии с ИНКОТЕРМС 2010)*	DDP термин употребляется с указанием места прибытия. Он означает, что ответственность продавца заканчивается после того, как товар доставлен в указанное место в стране покупателя. Все риски, все расходы по доставке груза (налоги, пошлины и т. д.), ответственность за порчу и потерю товара, включая пошлины и прочие выплаты, выплачиваемые при импорте, до этого момента несёт продавец, также он несёт ответственность за таможенную очистку.
Срок поставки*	В течении 16 календарных дней после получения заявки от Заказчика
Размер авансового платежа*	0 %
Наименование национальных стандартов, а при их отсутствии межгосударственных стандартов на закупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров, с учетом нормирования государственных закупок.	
Год выпуска (Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора)	2026
Гарантийный срок (в месяцах)	12

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	Общие требования Межсетевой экран следующего поколения – 1шт. Оборудование должно быть новым, упакованным и ранее не использованным. Недопустимо оборудование, бывшее в употреблении, восстановленное, переработанное или каким-либо образом модифицированное. Производственный код на упаковке, должен совпадать с производственным кодом на самом оборудовании. В составе заявки на участие необходимо приложить детализованную техническую спецификацию с указанием парт-номеров и описания. Технические характеристики межсетевого экрана Требования к межсетевому экрану следующего поколения. Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа трафика и состояния приложений для отслеживания и управления сетевыми потоками. Решение должно поддерживать работу DHCP в режимах сервера и ретранслятора (relay). Решение должно поддерживать возможность работы в режиме Transparent (Bridge). Решение должно обеспечивать работу на втором уровне модели OSI (режим Bridge). В режиме Bridge решение должно поддерживать следующие функции: Межсетевой экран (Firewall); Система предотвращения и обнаружения вторжений (IPS/IDS); URL-фильтрация (URL Filtering); Защиты от ботнет-активности (Antibot); Антивирусная защита (Antivirus); Управление приложениями (Application Control); Инспекция зашифрованного трафика (HTTPS Inspection); Средства идентификации и контроля пользователей (Identity Awareness); Механизма «песочницы» для анализа и изоляции подозрительных объектов (Sandboxing). Решение должно поддерживать кластеризацию Active/Standby в режиме Bridge. Решение должно поддерживать высокую доступность шлюза с синхронизацией состояний сетевых соединений. Решение должно обеспечивать поддержку протокола IPv6. Решение должно поддерживать политику, основанную на механизмах QoS. Решение должно обеспечивать возможность гарантирования или ограничения пропускной способности, а также управления задержкой для определённого IP-источника, IP-назначения или сервиса. Решение должно поддерживать настройку правил QoS для VPN-трафика, включая возможность гибкого определения параметров приоритезации, ограничения или гарантирования пропускной способности. Решение должно обеспечивать функционал Системы предотвращения вторжений (IPS). Система IPS должна обеспечивать обнаружение угроз на основе следующих механизмов: Сигнатурный анализ для выявления известных атак и эксплойтов; Отслеживание и анализ аномалий протоколов для выявления нестандартного или вредоносного трафика; Управление приложениями для контроля и блокировки нежелательной активности приложений; Обнаружение на основе анализа поведения для выявления ранее неизвестных атак и аномального поведения. Решение должно обеспечивать функционал интегрированной системы предотвращения вторжений (IPS) для защиты веб-приложений от вредоносного кода и атак. Система должна обеспечивать блокировку сетевых червей, атак переполнения буфера, SQL-инъекций, инъекций команд, межсайтового скриптинга (XSS), а также поддерживать настраиваемый модуль блокировки HTTP-червей. Дополнительно система должна обеспечивать защиту от обхода каталогов (Directory Traversal), вредоносных или некорректных HTTP-заголовков (Header Rejection), а также от вредоносного HTTP-кода. Решение должно обеспечивать функционал Идентификации и контроля пользователей. Должно обеспечивать возможность получения идентификаторов пользователей путем анализа событий безопасности Microsoft Active Directory. Должно поддерживать аутентификацию пользователей по идентификатору с использованием браузера, предназначенную для устройств и пользователей, не являющихся частью домена. Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности. Решение должно обеспечивать функционал Управления приложениями и веб-фильтрации (Application Control и URL-Filtering). База данных управления приложениями должна содержать более 10000 известных приложений. Решение должно обеспечивать детальный контроль безопасности минимум для 255000 Web 2.0 виджетов. Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL. Решение должно обеспечивать функционал защиты от ботнет-активности и антивирусной защиты (Anti-Bot и Antivirus). Приложение Anti-Bot должно быть способно выявлять аномальное сетевое поведение, указывающее на возможное заражение ботнетом, и обеспечивать автоматическую остановку такой активности. Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи, а также иметь механизмы, применяющие интеллектуальную аналитику для автоматической защиты от атак в протоколе DNS, включая механизмы защиты от DGA. Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам, а также обнаруживать и блокировать входящие вредоносные файлы. Приложение Anti-virus должно быть способно проверять шифрованный SSL трафик. Решение должно обеспечивать функционал инспекции SSL трафика. Решение должно обеспечивать функционал Песочницы (Sandboxing) (инспекция в облаке или на выделенном локальном устройстве) при наличии лицензии. Функционал «песочницы» должен обеспечивать защиту от атак нулевого дня (0-day attacks), а также от ранее неизвестного вредоносного программного обеспечения. Система обязана гарантировать предотвращение таких угроз в период до выпуска и распространения соответствующих статических сигнатур. Топология внедрения песочницы: Поддержка режима сетевой песочницы (Network-based); Поддержка режима работы в разрезе трафика - Inline (Bridge mode); Поддержка режима почтового агента (Mail transfer agent); Поддержка режима анализа зеркального трафика (TAP/SPAN порт). Решение не должно содержать раздельную инфраструктуру для защиты электронной почты и веб-трафика. Решение должно поддерживать кластеризацию для обеспечения отказоустойчивости. Решение должно поддерживать функционал эмуляции различных типов файлов, в том числе исполняемых файлов, архивов и документов, а также поддерживать эмуляцию Java и Flash. Движок эмуляции должен поддерживать различные операционные системы, включая Windows XP, 7, 8.1, 10 и 11, а также обеспечивать возможность использования специально настроенных образов (Customized images). Движок эмуляции должен обеспечивать функции инспекции, эмуляции и предотвращения вредоносной активности, а также обеспечивать передачу событий в инфраструктуру защиты от зловредного программного обеспечения. Решение должно обеспечивать эмуляцию файлов как небольшого размера, так и размером до 100 Мбайт. Решение должно обнаруживать атаки на стадии эксплуатации уязвимости (exploitation), предотвращая запуск шелл-кода (shell code) и исключая возможность загрузки либо исполнения вредоносного программного кода. Решение должно обеспечивать обнаружение ROP (Return Oriented Programming) и других техник эксплуатации уязвимостей, включая эскалацию привилегий (Privilege Exploitation), посредством мониторинга выполнения последовательности инструкций центрального процессора. Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня (0-day attacks) и неизвестного вредоносного программного обеспечения. Решение должно обеспечивать устойчивость к попыткам обнаружения песочницы со стороны вредоносного кода и содержать средства борьбы с методами обнаружения исполнения в изолированной среде. Решение должно обеспечивать возможность интеграции с централизованной системой управления и обеспечивать администрирование, настройку политик безопасности и мониторинг в единой точке. Решение должно генерировать подробный отчет по результатам анализа каждого зараженного файла. Решение должно поддерживать механизм мгновенной доставки безопасной копии документа, классифицированного как потенциально опасный, при этом оригинальный документ подлежит дальнейшему анализу и проверке. Решение должно поддерживать следующие технологии очистки документа от потенциальных угроз: Конвертация в PDF с сохранением исходного форматирования, нейтрализацией ссылок, возможностью выделения и копирования текста; Конвертация с сохранением исходного формата и удалением активного контента: скрипты, макросы, активные ссылки, вложенные объекты, нестандартные и стандартные поля. Решение должно поддерживать Веб-портал самообслуживания для запроса исходных файлов пользователями после проверки их в «песочнице». Решение должно обеспечивать гибкие настройки по поддержке оригинального формата файлов и указания тех видов контента, который должен быть удален. Решение должно обеспечивать блокировку в режиме реального времени неизвестного вредоносного программного обеспечения (пациента-0) при обращении к веб-ресурсам. Решение должно обеспечивать блокировку в режиме реального времени неизвестного вредоносного программного обеспечения (patient-zero), распространяемого через электронную почту. Решение должно обеспечивать функционал IPSec VPN. Решение должно поддерживать использование как встроенного центра сертификации (CA), так и внешних сторонних центров сертификации. Решение должно поддерживать шифрование 3DES и AES-256 для IKEv2 (фазы I и II), а также алгоритмы "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II. Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20. Решение должно поддерживать как минимум следующие механизмы обеспечения целостности данных с использованием алгоритмов: MD5, SHA-1 SHA-256, SHA-512 и AES-XCBC. Решение должно поддерживать реализацию VPN соединений типа Site-to-Site в следующих сетевых топологиях: Полносвязная сеть (все-со-всеми); Звездообразная сеть (удаленные офисы к центральному сайту); Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт). Решение должно обеспечивать Удаленный мобильный доступ Решение должно обеспечивать функционал Удаленного мобильного доступа минимум для 200 одновременных соединений пользователей. Решение должно обеспечивать поддержку двухфакторной аутентификации как через интеграцию с внешними системами двухфакторной аутентификации, так и посредством встроенного механизма двухфакторной аутентификации, предоставляемого производителем. Решение должно предоставлять следующие возможности: Безопасный доступ пользователей через VPN; Идентификация и привязка мобильных устройств к конкретным конечным пользователям для контроля доступа; Обеспечение соответствия подключаемых конечных точек требованиям корпоративной политике безопасности. Решение должно иметь встроенный функционал SD-WAN. Решение должно предоставлять функционал специализированных сервисов, предназначенных для защиты IoT устройств (при наличии дополнительной лицензии). Технические требования к шлюзу Продуктивные сетевые интерфейсы (минимальные требования): 8 x 1 Гбит/с LAN RJ-45 порт; 1 x 1 Гбит/с WAN RJ-45 порт; 1 x 1 Гбит/с DMZ SFP порт; 2 x 10 Гбит/с LAN/WAN SFP+ порт; 1 выключатель питания. 1 x USB 3.0 Type-A. 1 консольного порта USB Type-C. 2 x Power Supply Connector. Пропускная способность Firewall: не менее 8990 Мбит/с. Пропускная способность IPS: не менее 6890 Мбит/с. Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): не менее 4990 Мбит/с. Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачный Sandbox): не менее 2490 Мбит/с. Межсетевой экран 1518B UDP не менее 15490 Мбит/с. Задержка брандмауэра (средняя) 24 µSec. Пропускная способность VPN AES-GCM 1452B: не менее 4490 Мбит/с. Новые соединения: не менее 62000 соединений/с. Одновременные соединения: не менее 2 миллионов. Поддержка и подписка. Техническая поддержка на 3 года от производителя, 7 x 24, гарантийная замена оборудования. Подписка сроком на 3 года от производителя, должны быть включены все необходимые подписки на сервисы безопасности.
Сопутствующие услуги (указываются при наличии) (монтаж, наладка, обучение, проверки и испытания товаров)	

Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о закупках (указываются при наличии) (потенциальный поставщик за не указание и непредставление указанных сведений не отклоняется)	

* сведения подтягиваются из плана закупок (отображаются автоматически).

Примечание:

1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.

2. Квалификационные требования, предъявляемые потенциальным поставщикам в иных документах не устанавливаются.