Конкурстық құжаттамаға
13-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасы Президенті Іс басқармасының "Бурабай" мемлекеттік ұлттық табиғи паркі" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасы Президенті Іс басқармасының "Бурабай" мемлекеттік ұлттық табиғи паркі" мемлекеттік мекемесі
Конкурстың №:	№ 17942191-1
Конкурстың атауы:	Антивирустық бағдарламалық жасақтаманы сатып алу
Лоттың нөмірі:	№ 88370005-ОК2
Лоттың атауы	Бағдарламалық қамтамасыз ету
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*:	620129.000.000000
Тауардың атауы*:	Бағдарламалық қамтамасыз ету
Өлшем бірлігі*:	Дана
Саны (көлемі)*:	70
Қосылған құн салығын есептемегенде бірлік бағасы*:	24951.64
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома*:	1746614.8
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс*:	

Жеткізу шарттары (сәйкес ИНКОТЕРМС 2010)*	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*	Шарт күшіне енген күннен бастап 16 күнтізбелік күн ішінде. Өнім беруші Қазақстандық тауар өндірушілер тізілімінде болған жағдайда, жеткізу мерзімі - 61 күнтізбелік күн ішінде
Жеткізу орны*	117035100, Ақмола облысы, Бурабай ауданы, Бурабай к. ықшам Самал 3 өнеркәсіптік база
Аванстық төлем мөлшері*:	30
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.	ГОСТ Р 51188-2007
Тұрғын емес мақсаттағы ғимараттарды, құрылыстарды, үй-жайларды, авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған шарт жасасу күніне дейін (үш жылға дейін) шығарылған жылы болуға тиіс	
Кепілдік мерзімі (айлармен)	12

Сатып алынатын тауардың талап етілетін функционалдық, техникалық, сапалық, пайдалану және өзге де сипаттамаларының сипаттамасы	1.1. Лицензияны белсендірген күннен бастап кемінде 1 жылдық жазылым мерзімі бар, техникалық қолдау көрсетілетін 70 құрылғыға (соңғы нүктелерге) арналған оқиғаларды тергеу модулімен антивирустық қорғаныс (бұдан әрі «АҚ» деп аталады). 1.2. Әлеуетті жеткізуші тендерге ұсынылған бағдарламалық жасақтамаға лицензияланған бағдарламалық жасақтаманы өндірушіден немесе оның Қазақстан Республикасындағы өкілдігінен тендер шеңберінде тауарларды (қызметтерді) жеткізу құқығын беретін рұқсат хатын ұсынуы тиіс. Рұқсат хатын компанияның фирмалық бланкісінде, уәкілетті тұлғаның мөрі мен қолы басылған күйінде беруі тиіс; 1.3. Автоматтандырылған басқару жүйесін пайдалану құқығына берілген лицензия кейінге қалдырылған белсендіруді қолдауы тиіс. Лицензияны белсендіру өндірушіден жөнелтілген кезде автоматты түрде болмауы немесе алдын ала белгіленген күнге байланыстырылмауы тиіс. Лицензия жеткізушіден жөнелтілгеннен кейін екі (2) ай ішінде кез келген уақытта белсендірілуі тиіс. 1.4. Бағдарламалық жасақтаманы енгізу және конфигурациялау кезеңінде жеткізуші берілген АҚ-дың толық функционалдығы бар уақытша лицензияларды енгізуді аяқтауға жеткілікті мерзімге (тапсырыс берушімен келісім бойынша), бірақ 10 жұмыс күнінен аспайтын мерзімге беруге міндетті. 1.5. Бағдарламалық жасақтама жеткізуші мен өндірушінің техникалық қолдауымен қамтамасыз етілуі тиіс. Техникалық қолдау қашықтан (онлайн, қашықтан кеңес беру, телефон, электрондық пошта немесе арнайы портал арқылы) көрсетіледі. Бағдарламалық жасақтаманы қолдау мерзімі - 12 айды құрайды. 2.1. Антивирустық қорғаныс (бұдан әрі «АҚ» деп аталады) – бұл виртуалды құрылғы ретінде жеткізілетін, жергілікті жерде орнатылған бірыңғай басқару консолі бар, барлық кіріктірілген қорғаныс модульдері бірыңғай виртуалды құрылғыда қосымша үшінші тарап бағдарламалық жасақтамасын орнатуды болдырмау үшін немесе бұлтта қолжетімді болатын масштабталатын шешім, ол кез келген жерде кез келген түрдегі кез келген сандағы соңғы нүктелер үшін қауіпсіздік саясатын орналастыру, сәйкестік және басқару үшін бірыңғай нүктені қамтамасыз етеді. 2.2 Масштабтау мақсатында шешімде дерекқор қызметтері, байланыс қызметтері, жаңартулар және веб-қызметтер үшін арнайы компоненттер болуы керек. 2.3. Жергілікті орнатылған АҚ бірыңғай, конфигурацияланған виртуалды құрылғы (виртуалды кескін) ретінде жеткізілуі керек. Қолдау көрсетілетін виртуалдандыру платформаларына VMware, Microsoft, Red Hat, ядроға негізделген немесе KVM виртуалды машиналары, Oracle VM және Nutanix кіруі керек. Виртуалды құрылғы негізгі виртуалдандыру платформаларымен (OVA, XVA, VHD, OVF, RAW) үйлесімді бірнеше форматта қолжетімді болуы керек. 2.4. АҚ бірнеше виртуалды құрылғылар мен нақты рөлдердің бірнеше даналары үшін конфигурацияны қолдауы керек және сенімділік пен масштабталуды қамтамасыз ету үшін кіріктірілген жүктеме теңгергіші болуы керек. 2.5. Қауіпсіз орта үшін АҚ бірнеше виртуалды құрылғылар арасында қауіпсіз байланыс үшін VPN кластерін құруды қолдауы керек. 2.6. Әкімші тіркелгісі үшін қосымша

	қауіпсіздікті қамтамасыз ету үшін АҚ екі факторлы аутентификацияны қолдауы керек. 2.7. АҚ жалпы қауіпсіздікке, жаһандық қауіпсіздік қатерлеріне және виртуалды немесе физикалық компьютерлер мен серверлерді қорғайтын барлық қауіпсіздік модульдерін бақылауға оңай қол жеткізуді және басқаруды қамтамасыз ететін бірыңғай басқару нүктесінен - веб-консольден басқарылуы керек. 2.8. Антивирустық қорғау қолданыстағы зиянды бағдарламаларға қарсы шешімді қашықтан орналастыру және жою, сондай-ақ қашықтан сканерлеу тапсырмаларын конфигурациялау және іске қосу мүмкіндігіне ие болуы керек. 2.9. Веб-консоль басқарылмайтын жұмыс үстелдерін, Microsoft Active Directory, VMware vCenter, Citrix XenServer, VMware Tanzu, Veeam Backup & Replication және желіде оңай табылған серверлерді қорғауды жеңілдету және автоматты түрде қолдану үшін қолданыстағы басқару және мониторинг жүйелерімен интеграциялануы керек. 2.10. Веб-сервер лицензияланған сертификаттау органы немесе олардың өз ұйымы берген орталық басқару консолінен сандық сертификаттарды импорттауға мүмкіндік беруі керек. Сертификатты импорттау интуитивті болуы және орталық басқару консолінен орындалуы керек. 2.11. Шешім орталық консольде сертификат туралы ақпаратты көрсете алуы керек: атауы, берген органы, берілген күні және берілген сертификаттардың жарамдылық мерзімі. 2.12. Антивирустық қорғаныс соңғы нүкте қауіпсіздігінің бірнеше деңгейін қамтамасыз етуі керек: мінез-құлықты бақылаумен зиянды бағдарламалардан қорғау, нөлдік күндік қауіптен қорғау, қолданбалардың қара тізіміне енгізу және шектеулі ортадағы ықтимал қауіпті нысандарды оқшаулау, брандмауэр, құрылғыны басқару, мазмұнды басқару және фишингке қарсы қорғаныс. 2.13. Антивирустық бағдарламада кіріктірілген жүктеме теңгергіші болуы керек. 2.14. АҚ архитектурасының орталық логикасы үшінші тарап лицензиялық кілтін қажет етпей, ендірілген реляциялық емес дерекқорды және белгілі бір соңғы нүктелер санынан асатын орналастыру құралдарын пайдалануы тиіс. 2.15. Антивирустық құралдар келесі қауіпсіздік қызметтерін қамтуы керек: Соңғы нүктені қорғау; Виртуалды ортаны қорғау; Антивирустық бағдарлама пайдаланушы әрекеттерін сәйкестікке жазып алуы керек. Антивирустық бағдарламада әрбір пайдаланушы әрекеті үшін егжей тегжейлі журналдар болуы керек. Антивирустық бағдарлама аудит журналын іздеудің күрделі әдістерін қолдауы керек. 2.16. АҚ физикалық және виртуалды машиналар үшін бірыңғай саясат үлгісін және кез келген орта (физикалық немесе виртуалды) үшін бірыңғай орнатушыны пайдалануы керек, және АҚ Linux жүйесінде жұмыс істейтін физикалық нүктелерге (серверлер мен жұмыс станциялары) қолжетімді болуы керек. 2.17. АҚ келесі сканерлеу жүйелерін қамтуы керек. Орнату пакеттерін жасаған кезде сканерлеу жүйесі автоматты түрде орнатылуы керек, бұл соңғы нүкте агенттеріне машина конфигурацияларын анықтауға және сканерлеу технологияларын сәйкесінше бейімдеуге мүмкіндік береді. Әкімші сонымен қатар бірнеше сканерлеу технологияларының бірін таңдау арқылы сканерлеу жүйесін теңшей

	алады: 2.17.1. Жергілікті сканерлеу, мұнда сканерлеу соңғы нүктеде орындалады. 2.17.2. Орташа топтар үшін гибридті сканерлеу (жеке бұлт) бұлтты сканерлеуді және ішінара жергілікті қолтаңбаларды пайдаланады. 2.17.3. Шағын топтарға арналған жеке бұлттағы орталықтандырылған сканерлеу сканерлеу жұмыс жүктемелерін соңғы нүктелерден арнайы қауіпсіздік серверлеріне түсіру арқылы соңғы нүктені қорғауды оңтайландырады. Бұл сканерлеу үшін қауіпсіздік серверін қажет етеді. Бұл жағдайда қолтаңбалар жергілікті түрде сақталмайды және сканерленген файлдар қауіпсіздік серверіне жүктеледі. 2.18. Зиянды бағдарламалардан қорғау жүйесі келесі қорғау модульдерін қамтуы тиіс: 2.18.1. Зиянды бағдарламалардан қорғау Зиянды бағдарламалардан қорғау модулі қолтаңбалық, эвристикалық және мінез-құлықтық талдауды қолдана отырып, барлық қауіп түрлерін (вирустар, құрттар, трояндар, тыңшылық бағдарламалар, жарнамалық бағдарламалар, пернетақталарды ашушылар, руткиттер және т.б.) көп деңгейлі анықтауды және алдын алуды қамтамасыз етуі тиіс. 2.18.2. Кеңейтілген қауіп-қатерді бақылау Тіпті эвристикалық қозғалтқыштан да жалтаратын қауіп-қатерлерге арналған қорғаныстың үшінші деңгейі Кеңейтілген қауіп-қатерді бақылау түрінде қамтамасыз етіледі. Кеңейтілген бақылау жұмыс істеп тұрған процестерді үздіксіз бақылайды және күдікті әрекеттерді, мысалы, процесс түрін жасыру әрекеттерін, процестің жад кеңістігінде кодты орындауды (артықшылықты эскалация үшін жадты басып алу), репликацияны, файлды жылжытуды, процестер тізімінде жасыруды және тағы басқаларды бағалайды. Әрбір күдікті әрекет процестің рейтингін арттырады. Шекті мәнге жеткенде, ескерту іске қосылады. Бұл модуль тек қолдау көрсетілетін Windows жұмыс үстелі және сервер операциялық жүйелері үшін қолжетімді.. 2.18.3. Кеңейтілген Антиэксплойт Машиналық оқытуға негізделген, Advanced Anti-Exploit технологиясы анықтау қиын эксплойттарды пайдаланатын нөлдік күндік шабуылдарды бұғаттау керек. Advanced Anti-Exploit нақты уақыт режимінде соңғы эксплойттарды бақылап, қолданыстағы қауіпсіздік шешімдерін айналып өту үшін пайдаланылуы мүмкін жадтың бұзылуына байланысты осалдықтарды жоюы керек. Технология браузерлер, Microsoft Office және Adobe Reader және басқалары сияқты көптеген стандартты қолданбаларды қорғауы керек. Модуль жүйелік процестерді бақылап, қауіпсіздік тесіктерінен және қолданыстағы процестерді басып алудан қорғауы керек. 2.18.4. Бұзуға қарсы әрекет Қауіпсіздік агентінің тұтастығын бұзу үшін пайдаланылуы мүмкін соңғы нүктедегі осал драйверлерді анықтауы керек. Windows және Linux операциялық жүйелерімен үйлесімді болуы керек. 2.18.5. Бұзушылықтан кейінгі Қауіпсіздік агентінің кері шақыруларының түпкі нүктеде зиянды түрде жойылғанын немесе өшірілгенін анықтау керек, нәтижесінде тұтастық бұзылады. Windows операциялық жүйелерімен үйлесімді болуы керек. 2.18.6. Брандмауэр Брандмауэр қолданбалардың желіге және интернетке кіруін басқаруы керек. Қолжетімділік белгілі, заңды қолданбалардың дерекқорына негізделіп, автоматты түрде рұқсат

	етілуі керек. Сонымен қатар, брандмауэр жүйені портты сканерлеуден қорғауы, интернет қосылымын ортақ пайдалануды (ICS) шектеуі және жаңа түйіндер Wi-Fi арқылы қосылған кезде ескертуі керек. 2.18.7. Желілік шабуылдан қорғау Қауіпсіздік деңгейі - бұл күш қолдану шабуылдары, желілік эксплойттар, құпия сөз ұрлаушылар, диск арқылы жүктеулер, боттар және трояндар сияқты әдістерді қолдана отырып, соңғы нүктелерге қол жеткізуге бағытталған желілік шабуылдарды анықтауға арналған. 2.18.8. Мазмұнды басқару Мазмұнды басқару модулі рұқсат етілген трафикке, веб-қатынасқа, деректерді қорғауға және қолданбаларды басқаруға қатысты компания саясатының сақталуын қамтамасыз етуі керек. Әкімшілер трафикті сканерлеу параметрлері мен ерекшеліктерді орнатуға, веб-қатынасты жоспарлауға, белгілі бір веб-мекенжайларды немесе санаттарды бұғаттауға немесе рұқсат беруге, деректерді қорғау ережелерін конфигурациялауға және белгілі бір қолданбалар үшін рұқсаттарды орнатуға қабілетті болуы керек. 2.18.9. Құрылғыны басқару Құрылғыны басқару модулі құрылғылардың кең ауқымына (мысалы, USB флэш дискілері, Bluetooth құрылғылары, CD/DVD ойнатқыштары, сақтау құрылғылары және т.б.) арналған саясаттарды пайдалана отырып, блоктау ережелері мен ерекшеліктерді қолдану арқылы соңғы нүктелерге қосылған сыртқы құрылғылар арқылы маңызды деректердің ағып кетуіне және зиянды бағдарламалардың енуіне жол бермеуі керек. 2.18.10. Антивирустық агентті қорғауды жергілікті түрде өзгерту Басқару орталығының әкімшілері қауіпсіздік саясатының параметрлерін пайдаланып, стандартты соңғы нүкте пайдаланушыларына артықшылықты пайдаланушы құқықтарын бере алады. Бұл модуль әкімшілік пайдаланушы құқықтарын беруге мүмкіндік беруі керек, бұл соңғы пайдаланушыларға жергілікті консольді пайдаланып қауіпсіздік параметрлеріне кіруге және өзгертуге мүмкіндік береді. 2.18.11. Құмсалғыш Құмсалғыш антивирустық қозғалтқыштармен қол қойылмаған күдікті файлдарды автоматты және терең талдау арқылы соңғы қауіптерден қорғаудың жоғары деңгейін қамтамасыз етуі керек. Құмсалғыштың қауіпсіз ортасы оқшауланған виртуалды ортада пайдалы жүктемелерді орындау, олардың әрекетін талдау және вирусты немесе зиянды ниетті көрсетуі мүмкін ең аз жүйелік өзгерістер туралы хабарлау үшін кешенді технологиялар жиынтығын пайдалануы керек. 2.18.12. Exchange қорғауы Зиянды бағдарламалардан, антиспамнан, антифишингтен, мазмұнды сүзуден және электрондық пошта мазмұнын сүзуден Exchange қорғауын қамтамасыз етуі, қауіпсіз хабар алмасу ортасын қамтамасыз ету және өнімділікті жақсарту үшін Microsoft Exchange серверлерімен толық интеграциялануы керек. Танылған зиянды бағдарламаларға қарсы және антиспам технологияларын пайдалана отырып, бағдарлама Exchange пайдаланушыларын ең соңғы, ең күрделі зиянды бағдарламалардан және құпия және құнды пайдаланушы деректерін ұрлау әрекеттерінен қорғауы керек. 2.18.13. Оқиғаларды тергеу модулі Бұл күрделі қауіптерді немесе белсенді шабуылдарды анықтауға арналған оқиға корреляциясының компоненті. Корпоративтік интеграцияланған

	платформаның бөлігі ретінде, оқиғаларды тергеу модулі корпоративтік желіде жұмыс істейтін барлық құрылғылардың мүмкіндіктерін біріктіруі керек. Бұл компонент төтенше жағдайларға жауап беру топтары елеулі қауіптерді анықтап, оларға жауап берген кезде көмектесуі керек. Соңғы нүктелерді пайдаланып, компьютер мен операциялық жүйе деректерін біріктіру үшін соңғы нүктелерді басқарудағы қауіпсіздік модулін белсендіре аласыз. Екі жақтан да метадеректерді жинау және өңдеу клиент-сервер платформасында жүргізілуі керек. Оқиғаларды тергеу модулі анықталған оқиғалар туралы егжей-тегжейлі ақпаратты, интерактивті оқиға картасын, қалпына келтіру әрекеттерін және құм жәшігімен және кеңейтілген шабуылды анықтау модулімен интеграцияны қамтамасыз етуі керек. 3. Физикалық және виртуалды соңғы нүктелердегі антивирустық қорғау бағдарламалық жасақтамасына қойылатын талаптар Жұмыс станциясының антивирустық қорғау бағдарламалық жасақтамасы келесі функцияларды қамтамасыз етуі керек: 3.1. Amazon EC2 және Microsoft Azure бұлттық платформаларымен интеграция; 3.2. API кілттерін пайдаланып, үшінші тарап бағдарламалық жасақтама жеткізушілерімен интеграция; 3.3. Антивирустық бағдарламалық жасақтама Microsoft сервер рөлдері (DNS, DHCP, AD, Exchange, SharePoint) үшін кіріктірілген ерекшеліктерді қамтамасыз етуі керек. 3.4. Резиденттік антивирустық мониторинг; 3.5. Пайдаланушы немесе әкімші пәрмені бойынша антивирустық сканерлеу; 3.6. Жоспарланған антивирустық сканерлеу; 3.7. Флэш-дискілерді анықтаған кезде сканерлеу; 3.8. Эвристикалық талдау негізінде белгісіз зиянды бағдарламалардан қорғау; 3.9. Қажет болған жағдайда антивирустық қорғауды өшіру мүмкіндігі; 3.10. Клиент жұмыс станциясынан бағдарламаны жою үшін құпия сөз орнату мүмкіндігі; 3.11. Жасырын процестерді анықтау; 3.12. Операциялық жүйені жоспарланған тапсырманы іске қосу және/немесе дереу іске қосу; 3.13. Антивирустық бағдарламалық жасақтаманың тек таңдалған компоненттерін орнату мүмкіндігі; 3.14. Агентті қайта орнатпай немесе жоймай, әкімші консолі арқылы клиенттік компьютерде антивирустық агентті қашықтан қайта конфигурациялау, қорғаныс модульдерін қосу немесе өшіру мүмкіндігі. 3.15. Зиянды бағдарламалардың соңғы нүктеге енуіне жол бермеу үшін кіріс электрондық пошта хабарламаларын (POP3, IMAP, MAPI) және веб-трафикті нақты уақыт режимінде сканерлеу. 3.16. Зиянды бағдарламалардың басқа соңғы нүктелерге жұқтыруына жол бермеу үшін шығыс электрондық пошта хабарламаларын (SMTP, MAPI) сканерлеу. 3.17. Зиянды бағдарламаларды сканерлеуден белгілі бір трафик түрлерін алып тастау; 3.18. Белгілі бір процестерді немесе қолданбаларды сканерлеуден алып тастау; 3.19. Анықталған кезде анти-exploit сканерлеу және өңдеуден қорғау әрекеттері үшін қолданбаларды қосу және өңдеу; 3.20. Желілік шабуылдардан қорғау режимдерін өңдеу; 3.21. Блокталған немесе рұқсат етілген веб сайттардың тізімін жасау арқылы веб-ресурстарға кіруді басқару; 3.22. Белгілі бір уақыт аралығында немесе кестеге сәйкес пайдаланушыларға немесе қолданбаларға веб-кіруге

	рұқсат беру немесе тыйым салу; 3.23. Санатқа негізделген веб-сүзгінің болуы (веб-сайттарға олардың мазмұнына негізделген кіруді динамикалық сүзгілеу) 3.24. Пайдаланушылардың онлайн алаяқтарға кездейсоқ жеке немесе құпия ақпаратты жария етуіне жол бермеу үшін белгілі фишингтік веб беттерді автоматты түрде бұғаттайтын фишингке қарсы қорғаныстың болуы; 3.25. Келесі жабдық түрлерін бұғаттауға арналған құрылғыны басқару модулінің болуы, сондай-ақ нақты рұқсаттарды (рұқсат беру, бұғаттау, тек оқуға арналған, әкімші параметрлері) орнату мүмкіндігі Bluetooth құрылғылары, CD-ROM құрылғылары, дискеткалар, IEEE 1284.4, IEEE 1394, бейнелеу құрылғылары, модемдер, таспалы дискілер, портативті Windows құрылғылары, COM/LPT порттары, SCSI Raid, принтерлер, желілік адаптерлер, сымсыз желілік адаптерлер, ішкі және сыртқы сақтау орны; 3.26. Қолданбаларға арналған белсенді сүзу режимі, оны өшіру мүмкіндігін қоса алғанда; 3.27. Қажетсіз болуы мүмкін қолданбаларды сканерлеу; 3.28. Қауіпсіздік тіркелгі менеджерімен байланысты кілттерді қоса алғанда, маңызды тізілім кілттерін рұқсатсыз кіруден немесе пайдаланудан қорғау. 3.29. Ядро деңгейінде Windows API шақыруларын қосымша бақылау, бұл шабуыл тізбегінің басында кеңейтілген қауіптерді анықтау мүмкіндігін жақсартады. 3.30. Рұқсатсыз кіруден, рұқсатсыз бұзудан және ransomware бағдарламаларынан қорғау үшін Windows шифрлау файлдық жүйесінің деректерін қорғау модулінің болуы; 3.31. Бонус бағдарламалық жасақтамасын азайту (қалпына келтіру режимі сұраныс бойынша немесе автоматты түрде): 3.31.1. Соңғы нүктеде тікелей жұмыс істейтін процестерді басқару мүмкіндігі. 3.31.2. Қашықтан қолжетімді ортақ желілік ресурстарды бақылау мүмкіндігі. Бұл опцияны соңғы нүкте файлдық сервер болса немесе қолжетімді желілік ресурстар болса пайдалануға болады. 3.32. RDP қосылымын сканерлеу; 3.33. Шифрланған трафикті ұстап алу – HTTPS, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS 3.34. TLS қол алысуды ұстап алу 3.35. Шешім шығыс веб және электрондық пошта трафигін сканерлеу және бұғаттау мүмкіндігімен орталықтандырылған басқару консолі арқылы құпия деректерді қорғау ережелерін (мысалы, толық аты-жөні, телефон нөмірлері, банк деректемелері, PIN кодтары, электрондық пошта мекенжайлары) жасауды және конфигурациялауды қолдауы керек. Шешім пайдаланушыларды бұғаттау әрекеттері туралы хабардар етуі және ерекшеліктерді (сенімді мекенжайлар мен веб сайттар) конфигурациялауы керек; 3.36. Сенімді процестерді, файлдарды және қалталарды сканерлеуден шығару мүмкіндігі. 3.37. Орнату кезінде клиенттік жұмыс станцияларын үйлесімсіз бағдарламалық жасақтамаға алдын ала сканерлеу; 3.38. Жұмыс станцияларына клиентті орнату кезінде вирустар мен зиянды бағдарламаларға алдын ала сканерлеу; 3.39. Алдыңғы сканерлеуден бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету; 3.40. Тапсырма басымдығына байланысты антивирустық және басқа қолданбалар арасында жұмыс станциясы ресурстарын бөлуді реттеу: фонда антивирустық сканерлеуді жалғастыру мүмкіндігі;

	3.41. Қолданбаларды қара тізімге енгізу; 3.42. Антивирустық бағдарламаның егжей-тегжейлі жұмыс есептерін жасау; 3.43. Ақпаратты көрсетуді егжей-тегжейлі теңшеу және бүкіл ұйым бойынша жаппай әрекеттерді орындау мүмкіндігі бар егжей-тегжейлі, интерактивті басқару тақталарын жасау; 3.44. Басқару орталығының басты бетінде графиктер мен блок-схемалары бар кіріктірілген, жылдам есептер, оларды өңдеу және қосу мүмкіндігімен. 3.45. Соңғы нүкте мәселелерін шешуге арналған кіріктірілген қашықтан жөндеу мүмкіндігі. 4. Exchange антивирустық бағдарламалық жасақтамасына қойылатын талаптар 4.1. Электрондық пошталардың спам екенін анықтау үшін әртүрлі сүзгілер мен механизмдердің тіркесімдерін пайдалана отырып, спам мен фишингтен қорғаудың бірнеше деңгейлері; 4.2. Жаңа және белгісіз спам қауіптерін анықтауға арналған эвристикалық сүзгі. Сүзгі антиспам зертханасында спамның үлкен көлемі бойынша автоматты түрде оқытылуы керек. Оқыту кезінде ол бұрын талданған электрондық пошталарды пайдалана отырып, спам мен заңды хабарламаларды ажыратуды және өте нәзік ұқсастықтарға негізделген жаңа спамды тануды үйренуі керек. 4.3. Бұлтта үздіксіз дамып келе жатқан спам саусақ іздері дерекқорын жүргізу. Қолтаңбалары бар сұраулар бұлт серверлеріне жіберіліп, спамға дереу тексерілуі керек. Қолтаңбалар дерекқорда табылмаса да, оларды жақында алынған басқа сұраулармен салыстыру керек, ал белгілі бір шарттар орындалған жағдайда электрондық пошта спам ретінде белгіленуі мүмкін. 4.4. RBL сүзгісінің болуы; 4.5. Жіберушілердің ақ тізімдерінің болуы; 4.6. Спуфингке қарсы. 4.7. Exchange пошта серверін барлық зиянды қауіп түрлерінен (вирустар, трояндар, тыңшылық бағдарламалар, руткиттер, жарнамалық бағдарламалар және т.б.) вирус жұққан немесе күдікті нысандарды анықтау, оларды зарарсыздандыру әрекеті немесе көрсетілген әрекеттерге сәйкес вирус жұққан нысандарды оқшаулау арқылы қорғауға арналған зиянды бағдарламаларға қарсы модульдің болуы; 4.8. Тақырып, атау, тіркеме немесе көрсетілген өрнек бойынша поштаны бұғаттау; 5. Кіріктірілген құмсалғыш талаптары 5.1. Күдікті нысандарды соңғы нүктелерден құмсалғышқа терең мінез-құлық талдауы үшін автоматты және қолмен жіберу; 5.2. Пәрмен жолы аргументі арқылы үлгілерді қолмен тексеру мүмкіндігі; 5.3. URL мекенжайларын қолмен тексеру мүмкіндігі; 5.4. Машиналық оқыту және мінез-құлықты талдау; 5.5. Күдікті әрекетті анықтау және хабарлау; 5.6. Тәуекел индикаторларының ерте көрінуі; 5.7. Күдікті бағдарламалық жасақтаманы талдау режимдерінің қолжетімділігі: 5.7.1. Бақыланатын нысандар пайдаланушы үшін қолжетімді болып қалады. 5.7.2. Талдау нәтижесі қайтарылғанға дейін пайдаланушының нысанға кіруін бұғаттау тыйым салынады. 5.8. Құмсалғыш зиянды бағдарламалардың әрекеті туралы егжей-тегжейлі есептермен түсінік беруі керек. 6. Оқиғаларды тергеу модулінің талаптары 6.1. Әрбір EDR агентінде соңғы нүктені үздіксіз бақылайтын және күдікті оқиғалар мен ақпаратты қауіпсіз түрде хабарлайтын оқиғаларды тіркеуші болуы керек. 6.2. Гибридті инфрақұрылымдардағы (жұмыс

	станциялары, серверлер немесе әртүрлі операциялық жүйелерді іске қосатын контейнерлер) бірнеше соңғы нүктелерді қамтитын кеңейтілген шабуылдарды анықтау мүмкіндігі. 6.3. Қауіпті талдау модулі қосымша тергеу және жауап беру үшін соңғы нүкте оқиғаларын жинап, басымдық беруі керек. 6.4. EDR күдікті файлдарды құм жәшігінде детонациялау үшін жіберуі керек, содан кейін құм жәшігінің шешімін EDR оқиғалары туралы есептерінде пайдалануы керек. 6.5. Нақты уақыттағы EDR басқару тақтасына кез келген құрылғыдан қол жеткізуге болады, осылайша әкімшілер ескертулер мен визуализацияларды көре алады, содан кейін қауіптерді зерттеп, оларға тиімді жауап бере алады. 6.6. EDR сенсоры агентке енгізіліп, соңғы нүкте мен қолданбаның әрекеті туралы есеп беру үшін деректерді жинап, өңдейді. 6.7. Қауіпсіздік аналитикасы, сенсор жинаған метадеректерді түсіндіру үшін қолданылатын артқы компонент. 6.8. Шешім шабуыл белгілерін анықтау үшін соңғы нүкте оқиғаларын бақылап, мұндай әрекетті анықтаған кезде оқиғаны бастауы керек. 6.9. Шешім MITRE шабуыл индикаторларына және өзінің қауіп туралы ақпаратына негізделген бастапқы сызықтарды жасай алуы керек. 6.10. Бастапқы сызықтан кез келген ауытқу оқиға ретінде тіркелуі керек. 6.11. Шешім белгілі бір уақыт аралығында сенсор анықтаған барлық қауіпсіздік оқиғаларын сүзуге, тергеуге және шаралар қолдануға көмектесетін құралдарды ұсыну арқылы оқиғаларды талдауды қолдауы керек. 6.12. Шешім қауіпсіздік оқиғасының қауіпті екеніне сенімділік дәрежесін көрсететін сенімділік ұпайын тағайындауы керек. 6.13. Шешім MITER ATT&CK; білім қорымен біріктірілуі және сәйкесінше қауіпсіздік оқиғаларын белгілеуі керек. 6.14. Қауіпсіздік оқиғаларын файл атаулары, IP мекенжайлары, хост атаулары немесе IOC арқылы іздеуге болады. Пайдаланушыға күрделі критерийлер негізінде өткен оқиғаларды көруге мүмкіндік беретін кеңейтілген іздеу функциясы да қамтамасыз етілуі керек. Алдын ала анықталған сұраулар қауіпсіздік оқиғаларын іздеудің пайдалы жағдайларына арналған. 6.15. Оқиғаға әсер етуге шолу және әрбір оқиға түйіні туралы егжей-тегжейлі ақпарат. 6.16. Уақыт шкаласы функциясы қауіпсіздік оқиғаларының дамуы туралы ақпаратты хронологиялық тәртіппен жинауы керек. 6.17. Функция ағымдағы қауіпсіздік оқиғасы кезінде шешім автоматты түрде қабылдайтын бұғаттау әрекеттері туралы ақпаратты жинауы керек. 6.18. Шешім MD5/SHA256 хэш мәндерін пайдаланып, файлдарды/процестерді блоктау тізіміне қосуы керек. Мұны қауіпсіздік оқиғасынан алуға немесе CSV файлынан импорттауға болады. 6.19. Шешім ортада процестердің жұмыс істеуін тоқтатуы керек. 6.20. Шешім файлды карантинге қоюы керек, сәйкес элементті сақтап, оның пайдалы жүктемесін орындауына жол бермеуі керек. 6.21. Шешім басқару консолімен байланысты сақтай отырып, хосттың желіден оқшаулануына мүмкіндік беруі керек. 6.22. Шешім шабуылдың желі бойынша таралуын болдырмау үшін тиісті файлды немесе процесті блоктау тізіміне қосуы керек. 6.23. Файлды ерекшелік ретінде қосу мүмкіндігі - зиянды емес файл үшін бұл мүмкіндік заңды

	әрекетті болдырмау үшін пайдаланылуы мүмкін. 6.24. Шешім қосымша зерттеу үшін ішкі компоненттерді және үшінші тарап шешімдерін пайдалануы керек: 6.24.1. VirusTotal 6.24.2. Sandbox 6.24.3. Google 6.25. Шешім шабуылдарды тез тергеу, сот-медициналық деректерді жинау және бұзушылықтарды жою үшін хостқа қашықтан қосылуы керек. Бұл белгісіздікті жояды және шабуылдан туындайтын жұмыстың тоқтап қалу уақытын айтарлықтай қысқартады. 6.26. Шешім уәкілетті пайдаланушыға/әкімшіге басқарылатын соңғы нүктелерге консольден тікелей қауіпсіз кіруге мүмкіндік беруі керек. 6.27. Қашықтағы соңғы нүктеге сәтті қосылғаннан кейін, қауіпті дереу жою немесе одан әрі тергеу үшін деректер жинау үшін операциялық жүйеде бірнеше арнайы қабық командаларын тікелей орындауға болады. 6.28. Шешім сонымен қатар алдын алу деңгейлері бұғаттаған қауіпсіздік оқиғаларын визуализациялауды қамтамасыз етуі керек. 6.29. Шешім API арқылы жауап әрекеттерін орындау мүмкіндігін қамтамасыз етуі керек. 7. Қолдау көрсетілетін операциялық жүйе талаптары 7.1. Windows операциялық жүйелері 7.1.1. Windows 11, 10, Windows Server 2022, 2019, 2016 7.1.2. AZ Windows Server Failover Cluster (WSFC) технологиясын қолдауы керек. 7.2. Linux операциялық жүйелері 7.3. Mac OS операциялық жүйелері 8. Ұйымның сыртқы цифрлық активтерін бақылаудың қосымша қызметіне қойылатын талаптар 8.1. Соңғы нүктелерді кешенді қорғауды қамтамасыз ету және оқиғаларды тергеу модулінің тиімділігін арттыру үшін, соңғы нүктелерге шабуылдардың айтарлықтай бөлігі ұйымның осал интернетке қолжетімді ресурстары (мемлекеттік қызметтер, қосалқы домендер, IP мекенжайлары, сертификаттар және көлеңкелі IT ресурстары) арқылы басталатынын ескере отырып, пакетке сыртқы шабуыл бетін анықтау және талдау қызметі кіреді. Нәтижелер тәуекелдерге басымдық беру және шабуылдан қорғау саясатын конфигурациялау үшін пайдаланылады. Бұл қызметке ұйымның сыртқы цифрлық активтерін бақылауға арналған бір реттік қызмет кіруі керек, оған электронды форматта аналитикалық есеп берілуі керек. Қосымша қызмет ұйымның интернетке қолжетімді активтерін табуды, түгендеуді және талдауды қамтамасыз етуі керек. 8.2. Қызмет мыналарды қамтуы тиіс: 8.2.1. Интернетке қосылған көлеңкелі АТ ресурстарын және осал активтерді, қосымшаларды, қосалқы домендерді, IP мекенжайларын, үшінші тарап бұлттық орталарын және мерзімі өткен сертификаттарды анықтау. 8.2.2. Үшінші тарап немесе жеткізу тізбегінің тәуекелдерін бағалау: Үшінші тарап жеткізушілеріне, серіктестеріне және мердігерлеріне тиесілі немесе басқарылатын сыртқы активтерді олардың қауіпсіздік тәуекелдерін бағалау үшін бақылау. 8.2.3. Шабуылдаушылар пайдалануы мүмкін осалдықтарды, дұрыс емес конфигурацияларды және басқа да осалдықтарды анықтау үшін анықталған активтерді сканерлеу. 8.2.4. Шабуылдар кезінде ұйымды немесе оның өнімдерін еліктеу үшін пайдаланылуы мүмкін ұқсас домендерді және ықтимал жалған домендерді анықтау. 8.3. Қызмет көрсетілгеннен кейін, Жеткізуші анықталған активтердің тізімін, анықталған осалдықтардың және

	тәуекелдердің сипаттамасын, шабуыл бетінің динамикасын және анықталған қауіптерді азайту бойынша ұсыныстарды қамтитын аналитикалық есеп беруге міндетті.
Ілеспе қызметтер (қажет болған жағдайда көрсетіледі) (тауарларды монтаждау, баптау, оқыту, тексеру және 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)	

Ескертпе:
1. Функционалдық, техникалық, сапалық, пайдалану, өзге де сипаттамалар, ілеспе қызметтер және орындаушыға қосымша шарттар бойынша әрбір талап жеке жолда көрсетіледі.
2. Осы техникалық ерекшелікте әлеуетті өнім берушіге қойылатын біліктілік талаптарын белгілеуге жол берілмейді.
3. Өзге құжаттарда техникалық ерекшелік талаптарын белгілеуге жол берілмейді.
*мәліметтер мемлекеттік сатып алу жоспарынан тартылады (автоматты түрде көрсетіледі).

Приложение 13
к конкурсной документации

Техническая спецификация закупаемых товаров (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Государственный национальный природный парк "Бурабай" Управления делами Президента Республики Казахстан"
Наименование организатора	Государственное учреждение "Государственный национальный природный парк "Бурабай" Управления делами Президента Республики Казахстан"
№ конкурса:	№ 17942191-1
Наименование конкурса:	Приобретение антивирусного программного обеспечения
Номер лота:	№ 88370005-ОК2
Наименование лота:	Программное обеспечение
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*:	620129.000.000000
Наименование товара*:	Программное обеспечение
Единица измерения*:	Штука
Количество (объем)*:	70
Цена за единицу, без учета налога на добавленную стоимость*:	24951.64
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*:	1746614.8
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 течение 16 календарных дней со дня вступления договора в силу. В случае нахождения поставщика в Реестре казахстанских товаропроизводителей, срок поставки – в течение 61 календарных дней
Место поставки товара*:	117035100, Акмолинская область, Бурабайский район, п.Бурабай мкр. Самал 3 промышленная база
Размер авансового платежа* **:	30 %
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.	ГОСТ Р 51188-2007
Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора за исключением приобретения здания, строения, сооружения, помещения, имеющих нежилое назначение, авиационной техники	
Гарантийный срок (в месяцах)	12

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	1.1. Антивирусная защита (далее – «АЗ») с модулем расследования инцидентов на 70 устройств (конечных точек) с предоставлением технической поддержки, срок подписки не менее 1 года с момента активации лицензии. 1.2. Потенциальный поставщик должен представить авторизационное письмо от производителя лицензионного программного обеспечения или его представительства в Республики Казахстан поставляемого на конкурс программного обеспечения на право поставки товаров (услуг) в рамках данного конкурса. Авторизационное письмо должно быть оформлено на фирменном бланке, с печатью и подписью уполномоченного лица; 1.3. Поставляемая лицензия на право использования АЗ должна поддерживать возможность отложенной активации. Активация лицензии не должна производиться автоматически по факту отгрузки от производителя или быть привязана к заранее определённой дате. Лицензия должна предоставлять возможность активации в любой день в течение 2 (двух) месяцев с момента отгрузки от поставщика. 1.4. На период внедрения и настройки программного обеспечения поставщик обязан предоставить временные лицензии с полным функционалом поставляемого АЗ на срок, достаточный для завершения внедрения (по согласованию с заказчиком), но не более 10 рабочих дней. 1.5. ПО должна обеспечиваться технической поддержкой от поставщика и производителя. Форма оказания технической поддержки дистанционно (онлайн, удалённые консультации, телефон, электронная почта, специализированный портал). Срок поддержки ПО - 12 месяцев. 2.1. Антивирусная защита (далее – «АЗ») должна представлять собой масштабируемое решение, с единой консолью управления поставляемое в качестве виртуального устройства, установленного локально, со всеми встроенными модулями защиты в одно виртуальное устройство для предотвращения установки дополнительного стороннего программного обеспечения или доступной в облаке, что должно обеспечивать единую точку для развертывания, соблюдение и управление политиками безопасности для любого количества конечных точек, любого типа, в любом месте. 2.2. В целях масштабируемости решение должно иметь выделенные компоненты для служб баз данных, служб связи, обновлений и веб-служб. 2.3. Локально установленная АЗ должна поставляться как единое настроенное виртуальное устройство (виртуальный образ). Поддерживаемыми платформами виртуализации должны быть VMware, Microsoft, Red Hat, виртуальная машина на основе ядра или KVM, Oracle VM, Nutanix. Виртуальное устройство должно быть доступно в нескольких вариантах, совместимых с основными платформами виртуализации (OVA, XVA, VHD, OVF, RAW). 2.4. АЗ должна поддерживать настройку на использование нескольких виртуальных устройств и множество экземпляров конкретных ролей, иметь встроенный балансировщик нагрузки, чтобы обеспечить надежность и масштабируемость 2.5. Для более безопасной среды АЗ должна поддерживать созданий VPN-кластера для связи по безопасному каналу между несколькими виртуальными устройствами. 2.6. АЗ должна поддерживать двух факторную аутентификацию для

	обеспечения дополнительной защиты учетной записи Администратора. 2.7. АЗ должна управляться из единой точки управления - веб-консоли, которая должна обеспечивать легкий доступ и управление общей безопасностью, глобальными угрозами безопасности и контроль над всеми модулями безопасности, защищающих виртуальные или физические компьютеры и сервера. 2.8. АЗ должна иметь возможности удаленного развертывания и удаления существующего решения для защиты от вредоносных программ, настраивать и запускать задачи удаленного сканирования 2.9. Веб консоль должна интегрироваться в существующие системы управления и системы мониторинга, чтобы упростить и автоматически применять защиту для неуправляемых настольных компьютеров, серверов которые появляются в Microsoft Active Directory, VMware vCenter, Citrix XenServer, VMware Tanzu, Veeam Backup & Replication и которые просто обнаружены в сети 2.10. Веб-сервер должен позволять импортировать цифровые сертификаты из центральной консоли управления, выданные лицензированным центром сертификации или их собственной организацией. Импорт сертификатов должен быть интуитивно понятным и выполняться с центральной консоли управления. 2.11. Решение должно иметь возможность отображать в центральной консоли информацию о сертификатах: имя, центр выдачи, дату выпуска и дату истечения срока действия выданных сертификатов 2.12. АЗ должна обеспечивать несколько уровней безопасности для конечных точек: защита от вредоносного ПО с мониторингом поведения, защита от угроз нулевого дня, составление черных списков приложений и изоляция потенциально опасных объектов в ограниченной среде, межсетевой экран, управление устройствами, управление контентом, антифишинг. 2.13. АЗ должна иметь встроенный балансировщик нагрузки. 2.14. Центральная логика архитектуры АЗ должна использовать встроенную не-реляционную базу данных, и средство для развертываний, превышающих определенное количество конечных точек, без необходимости использования стороннего лицензионного ключа 2.15. Антивирусные средства должны включать следующие службы безопасности: Защита конечных точек; Защита виртуальных сред; АЗ должна регистрировать действия пользователя на соответствие. АЗ должна иметь подробные журналы для каждого действия пользователя. АЗ должна поддерживать сложный поиск журналов аудита 2.16. АЗ должна использовать единый шаблон политики для физических и виртуальных машин, и один установщик для любых сред (физических или виртуальных), также АЗ должна быть доступной для физических конечных точек под управлением Linux (серверы и рабочие станции). 2.17. АЗ должна включать в себя следующие сканирующие движки Сканирующий движок должен автоматически устанавливается во время создания установочных пакетов, позволяя агентам конечных устройств определять конфигурации машин и соответствующим образом адаптировать технологии сканирования. Также администратор может подстроить сканирующий движок, выбирая между несколькими технологиями сканирования: 2.17.1. Локальное сканирование,

	когда сканирование выполняется на конечном устройстве 2.17.2. Гибридное сканирование (частное облако), для средних групп, использует сканирование в облаке и, частично, локальные сигнатуры. 2.17.3. Центральное сканирование в частном облаке для малых групп для оптимизации защиты конечных устройств путем переноса нагрузки по сканированию с конечных точек на специализированные серверы безопасности, требует для сканирования сервер безопасности. В этом случае сигнатуры не хранятся локально и сканирование выгружается на сервер безопасности. 2.18. АЗ должна включать в себя следующие модули защиты: 2.18.1. Защита от вредоносного ПО Модуль защиты от вредоносного ПО должен обеспечивать многоуровневое выявление и предотвращеание всех типов угроз (вирусы, черви, трояны, шпионское и рекламное ПО, кейлоггеры, руткиты и др.) с использованием сигнатурного, эвристического и поведенческого анализа. 2.18.2. Расширенный контроль угроз Для угроз, которые ускользают даже от эвристического движка, присутствует третий слой защиты в виде расширенного контроля угроз. Расширенный контроль угроз постоянно отслеживает запущенные процессы и оценивает подозрительное поведение, такое как: попытки замаскировать тип процесса, выполнение кода в пространстве памяти процесса (захват памяти для привилегированной эскалации), репликация, перемещение файлов, скрытность в списке технологических процессов и т.д. Каждое подозрительное поведение повышает рейтинг процесса. Когда достигается порог, включается сигнал тревоги. Этот модуль доступен только для поддерживаемых настольных и серверных операционных систем Windows. 2.18.3. Расширенный Anti-Exploit Основанная на машинном обучении, технология Advanced Anti-Exploit должна блокировать атаки нулевого дня, использующие трудно-обнаруживаемые эксплойты. Advanced Anti exploit в режиме реального времени должен отслеживать последние эксплойты и устранять уязвимости повреждения памяти, которые могут использоваться для обхода существующих решений безопасности. Технология должна защищать большинство стандартных приложений, таких как браузеры, редакторы Microsoft Office и Adobe Reader и другие. Модуль должен следить за системными процессами и защищать от брешей в безопасности и перехватов существующих процессов. 2.18.4. Анти-Тампериг Должен обнаруживать уязвимые драйверы на конечной точке, которые могут быть использованы для угрозы целостности агента безопасности. Должен быть совместим операционными системами Windows и Linux. 2.18.5. Пост-Тампериг Должен определять, были ли обратные вызовы агента безопасности злонамеренно удалены или отключены на конечной точке, что привело к нарушению целостности. Должен быть совместим с операционными системами Windows. 2.18.6. Брандмауэр Брандмауэр должен контролировать доступ приложений к сети и к Интернету. Доступ должен разрешается автоматически, основываясь на базе данных известных, легитимных приложений. Кроме того, брандмауэр должен защищать систему от сканирования портов, ограничивать использование общего

	доступа к Интернет (ICS) и предупреждать, когда новые узлы подключаются по Wi-Fi. 2.18.7. Защита от сетевых атак Уровень безопасности, предназначенный для распознания сетевых атак, целью которых является получение доступа к конечным точкам при помощи таких средств как: атаки методом перебора, сетевые "эксплоиты", программы для кражи паролей, векторы заражения посредством скрытой загрузки, боты и трояны. 2.18.8. Контроль контента Модуль Контентного Контроля должен обеспечивать соблюдение политики компании в отношении разрешенного трафика, веб-доступа, защиты данных и контроля приложений. Администраторы должны иметь возможность задавать параметры сканирования трафика и исключения, составлять график доступа к веб, блокировать или разрешать определенные веб-адреса или категории, настраивать правила защиты данных и устанавливать разрешения для использования конкретных приложений. 2.18.9. Контроль устройств Модуль Контроля устройств должен предотвращать утечки критических данных и проникновение вредоносного ПО через внешние устройства, подключаемые к конечным точкам, применяя блокирующие правила и исключения с помощью политик для широкого спектра устройств (таких, как USB флэш-накопители, устройства Bluetooth, CD/DVD-плееры, устройства хранения, и т.д.). 2.18.10. Локальное изменение защиты антивирусного агента Администраторы Центра управления (Control Center) могут предоставлять права привилегированных пользователей обычным пользователям конечных устройств с помощью параметров политики безопасности. Данный модуль должен разрешать предоставление администраторских прав уровню пользователей, которые разрешат конечным пользователям получать доступ и изменять настройки безопасности, используя локальную консоль. 2.18.11. Песочница Песочница должна обеспечивать мощный уровень защиты от новейших угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусными ядрами антивируса. Безопасная среда Песочницы должна использовать обширный набор технологий для выполнения полезных нагрузок в изолированной виртуальной среде, анализировать их поведение и сообщать о мельчайших системных изменениях, которые могут свидетельствовать о вирусной и злонамеренной природе файлов. 2.18.12. Защита Exchange Должна обеспечивать защиту Exchange от вредоносных программ, антиспам, антифишинг, фильтрацию контента и содержимого писем, полностью интегрироваться с серверами Microsoft Exchange, для обеспечения безопасной среды обмена сообщениями и повышения производительности. Использовать признанные технологии защиты от вредоносных программ и спама, программа должна защищать пользователей Exchange от новейших, самых сложных вредоносных программ и от попыток украсть конфиденциальные и ценные данные пользователей. 2.18.13. Модуль расследования инцидентов Это компонент корреляции событий, должен выявлять сложные угрозы или активные атаки. В рамках корпоративной интегрированной платформы модуль расследования инцидентов должен объединять возможности всех

	устройств, работающих в корпоративной сети. Этот компонент должен приходить на помощь в случаях, когда группы немедленного реагирования распознают и отвечают на серьезные угрозы. Посредством конечных точек вы можете активировать защитный модуль в управлении конечной точки, чтобы объединять данные компьютера и операционной системы. Сбор и обработка метаданных с обеих сторон должна идти на платформе клиент-сервер. Модуль расследования инцидентов должен предоставлять детальную информацию по обнаруженным происшествиям, интерактивной карте происшествий, действиям по исправлению и интеграции с песочницей и Модуль обнаружения передовых атак 3. Требования к программным средствам антивирусной защиты на физических и виртуальных конечных устройствах Программные средства антивирусной защиты рабочих станций должны обеспечивать реализацию следующих функциональных возможностей: 3.1. Интеграция с облачными платформами Amazon EC2, Microsoft Azure; 3.2. Интеграция со сторонними производителями ПО при помощи API ключей; 3.3. АЗ должна предоставлять встроенные исключения для ролей сервера Microsoft (DNS, DHCP, AD, Exchange, SharePoint). 3.4. Резидентный антивирусный мониторинг; 3.5. Антивирусное сканирование по команде пользователя или администратора; 3.6. Антивирусное сканирование по расписанию; 3.7. Запуск сканирования при обнаружении Flesh накопителей; 3.8. Защита от еще неизвестных вредоносных программ на основе эвристического анализа; 3.9. Функция отключения антивирусной защиты при необходимости; 3.10. Функция установки пароля на удаление программы с клиентской рабочей станции; 3.11. Обнаружение скрытых процессов; 3.12. Запуск задач по расписанию и/или сразу после загрузки операционной системы; 3.13. Функция установки только выбранных компонентов программного средства антивирусной защиты; 3.14. Возможность удаленной перенастройки антивирусного агента, добавление или отключение модулей защиты, на клиентской машине через консоль администратора без переустановки и удаления агента. 3.15. Сканирование входящих сообщений электронной почты (POP3, IMAP, MAPI) и веб-трафика проверка в режиме реального времени, для предотвращения проникновения вредоносного ПО в конечную точку. 3.16. Проверка исходящих сообщений электронной почты (SMTP, MAPI) для предотвращения заражения вредоносными программами других конечных точек. 3.17. Исключение определенного вида трафика из сканирования на наличие вредоносных программ; 3.18. Исключение из сканирования указанных процессов или приложений; 3.19. Добавление и редактирование приложений на проверку Anti-Exploit а также редактирования действий защиты при обнаружении; 3.20. Редактирование режимов защиты от сетевых атак; 3.21. Управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов; 3.22. Функция разрешения или запрета на веб-доступ пользователям или приложениям в определенные интервалы времени или по расписанию; 3.23. Наличие Веб-фильтра по категориям (динамическая фильтрация доступа к сайтам

	на основе их содержимого) 3.24. Наличие защиты от фишинга с автоматической блокировкой известных фишинговых веб-страниц, чтобы пользователи случайно не раскрыли частную или конфиденциальную информацию интернет-мошенникам; 3.25. Наличие модуля контроля устройств для блокировки следующих типов оборудования а также возможностью задавать определенные разрешения (разрешить, заблокировать, только чтение, настройка администратора) - устройства Bluetooth, устройства CD-ROM, дисковые накопители на гибких дисках, IEEE 1284.4, IEEE 1394, устройства обработки изображений, модемы, ленточные накопители, портативные Windows-устройства, порты COM/LPT, SCSI Raid, принтеры, сетевые адаптеры, беспроводные сетевые адаптеры, внутренние и внешние хранилища; 3.26. Активный режим фильтрации для приложений, а также возможность отключения; 3.27. Сканирование на наличие потенциально нежелательных приложений; 3.28. Наличие функции защиты критических ключей реестра, в том числе связанных с Security Account Manager, от несанкционированного доступа или эксплуатации. 3.29. Наличие дополнительной функции отслеживания вызовов Windows API на уровне ядра, что повышает способность обнаруживать сложные угрозы на ранних этапах цепочки атак. 3.30. Наличие модуля защиты данных Windows Encrypting File System от несанкционированного доступа, несанкционированного вмешательства и от программ-вымогателей; 3.31. Смягчение последствий вирусов вымогателей (Режим восстановления- По запросу или автоматически): 3.31.1. Возможность контроля процессов, которые выполняются непосредственно на конечной точке. 3.31.2. Возможность мониторинга общих сетевых ресурсов, доступ к которым осуществляется удаленно. Возможность использовать этот параметр, если конечная точка является файловым сервером или имеет доступные сетевые ресурсы. 3.32. Сканирование RDP подключений; 3.33. Перехват зашифрованного трафика – HTTPS, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS 3.34. Перехват TLS handshake 3.35. Решение должно поддерживать создание и настройку правил защиты конфиденциальных данных (например, ФИО, телефоны, банковские реквизиты, PIN-коды, адреса электронной почты) через централизованную консоль управления, с возможностью сканирования и блокировки исходящего веб- и почтового трафика. Решение должно обеспечивать уведомление пользователей о блокировке, настройку исключений (доверенные адреса и сайты); 3.36. Возможность исключить из проверки доверенные процессы, файлы и папки. 3.37. Предварительная проверка клиентской рабочей станции на несовместимое ПО при установке; 3.38. Предварительное сканирование на вирусы и вредоносное ПО при установке клиента на рабочие станции; 3.39. Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; 3.40. Регулировка распределения ресурсов рабочей станции между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; 3.41. Создания черных

	списков приложений; 3.42. Создание детализированных отчетов работы антивирусной программы; 3.43. Создание детализированных, интерактивных панелей с подробной настройкой отображения информации на них и возможностью массовых действий по всех организации; 3.44. Наличие встроенных, быстрых отчетов с графиками и блок схемами на главной странице центра управления, возможность их редактирования и добавления 3.45. Наличие встроенной функции удаленной отладки для устранения проблем на конечной точке 4. Требования к программным средствам антивирусной защиты Exchange 4.1. наличие нескольких защитных слоев против спама и фишинга, используя комбинации различных фильтров и механизмов, для определения являются ли письма спамом или нет; 4.2. наличие эвристического фильтра для обнаружения новых и неизвестных спам угроз. Фильтр должен автоматически обучается на больших объемах спама внутри антиспам-лаборатории. Во время обучения он должен учится различать спам и легитимные сообщения, распознавать новый спам на основе очень тонкого сходства, используя уже рассмотренную электронную почту 4.3. поддержка постоянно развивающейся базы данных "отпечатков" спам-почты в облаке. Запросы, содержащие характерные признаки, должны отправляться на облачные серверы и мгновенно проверяться, являются ли эти сообщения спамом. Даже если характерные признаки не найдены в базе данных, они должны сверяются с другими недавно полученными запросами, и при выполнении определенных условий, электронное сообщение может быть помечено как спам; 4.4. наличие фильтра RBL; 4.5. наличие белых списков отправителей; 4.6. Антиспуфинг; 4.7. Наличие модуля защиты от вредоносных программ для защиты почтового сервера Exchange от всех видов вредоносных угроз (вирусов, троянов, шпионских программ, руткитов, рекламного ПО, и т.д.), путем обнаружения зараженных или подозрительных объектов, попытками их лечения или путем изоляции инфицированных объектов, в соответствии с заданными действиями; 4.8. Блокировка почты по теме письма, названию, вложению, заданному выражению; 5. Требования к встроенной песочнице 5.1. наличие автоматической и ручной отправки подозрительных объектов из конечных точек в Песочницу для углубленного анализа поведения; 5.2. возможность ручной проверки образцов с аргументом командной строки; 5.3. возможность ручной проверки URL адресов; 5.4. машинное обучение и анализ поведения; 5.5. выявление и отчет о подозрительной деятельности; 5.6. получение ранней видимости индикаторов подверженных риску; 5.7. Наличие режимов анализа подозрительного ПО: 5.7.1. объекты, подвергшиеся мониторингу по-прежнему доступны для пользователя. 5.7.2. блокировка доступа пользователя к объекту отклоняется до тех пор, пока результат анализа не будет возвращен. 5.8. Песочница должна обеспечивать понимание поведения вредоносных программ с подробными отчетами 6. Требования к модулю расследования инцидентов 6.1. Каждый агент EDR должен иметь регистратор событий, который постоянно контролирует конечную точку и

	безопасно отправляет информацию и подозрительные события. 6.2. Возможность для обнаружения продвинутых атак с участием нескольких конечных точек в гибридных инфраструктурах (рабочих станциях, серверах или контейнерах, работающих под управлением различных ОС) 6.3. Модуль Анализа угроз должен собирать и распределять события конечных точек в приоритетный список инцидентов для дополнительного расследования и реагирования. 6.4. EDR должен отправлять подозрительные файлы для детонации в песочнице, а затем использовать вердикт песочницы в отчетах EDR об инцидентах. 6.5. Панель мониторинга EDR в режиме реального времени должна быть доступна с любого устройства, чтобы администраторы могли просматривать предупреждения и визуализации, а затем исследовать угрозы и эффективно реагировать на них. 6.6. Датчик EDR должен быть встроен в агент, собирать и обрабатывать данные для передачи данных о поведении конечных точек и приложений. 6.7. Аналитика безопасности, внутренний компонент, используемый для интерпретации метаданных, собранных датчиком. 6.8. Решение должно отслеживать события конечных точек в поисках признаков атаки и инициировать инцидент при обнаружении такой активности. 6.9. Решение должно иметь возможность создавать базовые системы на основе индикаторов атаки MITRE и собственной аналитики угроз. 6.10. Любое отклонение от базовой линии должно регистрироваться как инцидент. 6.11. Решение должно обеспечивать поддержку анализа инцидентов, предоставляя инструменты, помогающие фильтровать, исследовать и принимать меры в отношении всех событий безопасности, обнаруженных датчиком в течение определенного интервала времени. 6.12. Решение должно присваивать значение оценки достоверности, указывающее степень уверенности в том, что событие безопасности является опасным. 6.13. Решение должно интегрироваться с базой знаний MITRE ATT & CK и соответствующим образом маркировать события безопасности. 6.14. События безопасности можно искать по именам файлов, IP-адресам, именам хостов или IOC. Так же должна быть предоставлена функция расширенного поиска, которая позволяет пользователю просматривать прошлые события на основе сложного критерия. Предопределенные запросы предназначены для полезных случаев поиска событий безопасности. 6.15. Обзор влияния события и подробная информация о каждом узле события. 6.16. Функция временной шкалы должна собирать информацию о развитии событий безопасности в хронологическом порядке. 6.17. Функция сбора информацию о блокирующих действиях, автоматически предпринимаемых решением при текущем событии безопасности. 6.18. Решение должно добавлять файлы / процессы в список блокировки, используя хеш-значения MD5 / SHA256. Это можно сделать из инцидента безопасности или импортировать из файла CSV. 6.19. Решение должно останавливать выполнение процессов в среде. 6.20. Решение должно помещать файл в карантин, сохраняя соответствующий элемент и не позволяя ему выполнять свои полезные данные. 6.21. Решение должно позволять изолировать хост от

	сети, сохранив связь с консолью управления. 6.22. Решение должно добавлять в список блокировки соответствующий файл или процесс, чтобы предотвратить распространение атаки в сети. 6.23. Возможность добавить файл как исключение - для не вредоносного файла этот параметр можно использовать для исключения законной активности. 6.24. Решение должно использовать внутренние компоненты и сторонние решения для дальнейшего исследования: 6.24.1. VirusTotal 6.24.2. Песочница 6.24.3. Google 6.25. Решение должно удаленно подключаться к хосту для быстрого расследования атак, сбора криминалистических данных и устранения нарушений. Это устраняет неопределенность и значительно сокращает время простоя в результате атаки. 6.26. Решение должно позволять авторизованному пользователю / администратору получить безопасный доступ к управляемым конечным точкам прямо с консоли. 6.27. После успешного подключения к удаленной конечной точке несколько настраиваемых команд оболочки могут быть выполнены непосредственно в операционной системе для немедленного устранения угрозы или сбора данных для дальнейшего расследования. 6.28. Решение должно также обеспечивать визуализацию событий безопасности, которые блокируются превентивными уровнями. 6.29. Решение должно предоставлять возможность выполнять ответные действия через API. 7. Требование к поддерживаемым операционным системам 7.1. Операционные системы Windows 7.1.1. Windows 11, 10, Windows Server 2022, 2019, 2016 7.1.2. А3 должна поддерживать технологию отказоустойчивого Windows-кластера (Windows Server Failover Cluster - WSFC). 7.2. Операционные системы Linux 7.3. Операционные системы Mac OS 8. Требования к дополнительной услуге мониторинга внешних цифровых активов организации 8.1. В целях комплексной защиты конечных точек и повышения эффективности модуля расследования инцидентов, с учётом того, что значительная часть атак на конечные устройства начинается через уязвимые интернет-доступные ресурсы организации (публичные сервисы, субдомены, IP-адреса, сертификаты, теневые ИТ-ресурсы), в состав поставки включается услуга по выявлению и анализу внешней поверхности атаки, результаты которой используются для приоритизации рисков и настройки политик А3. В состав услуги должна входить единоразовая услуга по мониторингу внешних цифровых активов организации с предоставлением аналитического отчета в электронном формате. Дополнительная услуга должна обеспечивать обнаружение, инвентаризацию и анализ интернет доступных активов организации. 8.2. В рамках оказания услуги должно выполняться: 8.2.1. Выявление теневых ИТ-ресурсов, подключенных к Интернету и уязвимых активов, приложений, субдоменов, IP-адресов, сторонних облачных сред, просроченных сертификатов. 8.2.2. Оценка рисков, связанных со сторонними организациями или цепочкой поставок: Мониторинг внешних активов, принадлежащих или управляемых сторонними поставщиками, партнерами и подрядчиками, для оценки их рисков безопасности. 8.2.3. Сканирование обнаруженных активов на наличие уязвимостей,

	неправильных настроек или других уязвимостей, которые могут быть использованы злоумышленниками. 8.2.4. Выявление похожих доменов и потенциальных поддельных доменов, которые могут быть использованы для имитации организации или ее продуктов при атаках 8.3. По результатам оказания услуги Поставщик обязан предоставить аналитический отчет, содержащий перечень обнаруженных активов, описание выявленных уязвимостей и рисков, динамику изменений поверхности атаки, рекомендации по устранению выявленных угроз.
Сопутствующие услуги (указываются при необходимости) (монтаж, наладка, обучение, проверки и испытания товаров)	
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	

Примечание
1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.
2. Установление в настоящей технической спецификации квалификационных требований, предъявляемых к потенциальному поставщику, не допускается.
3. Установление требований технической спецификации в иных документах не допускается.
* сведения подтягиваются из плана государственных закупок (отображаются автоматически).