ТЕХНИКАЛЫҚ СИПАТТАМА

1031888 сатып алу бойынша
Бағалы ұсыныстарға сұраным тәсілімен

Лот № 5 (18 У, 3765662) Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Тапсырыс беруші: АҚ "Каражанбасмунай"

Ұйымдастырушы: АҚ "Каражанбасмунай"

1. ТЖҚ қысқаша сипаттамасы

Атауы	Мәні
Жол нөмірі	18 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер, Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Қосымша сипаттама	Виртуалды серверлерді қорғау жүйесіне жазылымына қол жеткізу қызметі
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Маңғыстау облысы, Ақтау Қ.Ә., Ақтау қ., мкр.9 А, БЦ Елес
Жеткізу шарттары	-
Жеткізу мерзімі	01.2025 бастап 03.2025 дейін (қоса алғанда)
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

2.1 Терминдер, қысқартулар және анықтамалар:

Қызметтер – Виртуалды серверлерді қорғау жүйесіне жазылымына қол жеткізу қызметі;

ОЖ – Операциялық жүйе;

Виртуалды машина, ВМ – виртуалды ортадағы нақты компьютер сияқты жұмыс істейтін виртуалды компьютер. Қарапайым тілмен айтқанда, бұл толыққанды операциялық жүйесі мен аппараттық құралы бар компьютерді имитациялайтын қосымша;

Виртуалды сервер – бұл виртуалды машина негізінде жұмыс істейтін сервер;

БЖ – Бағдарламалық жасақтама;

AD – Active Directory.

2.2 Жалпы талаптар.

Виртуалды серверлерге арналған антивирустық қорғаныс Windows және Linux ОЖ негізіндегі виртуалды машиналар мен серверлерді қорғауы керек. Шешім мыналарды қамтуы керек:

- виртуалды ортаға арналған агентсіз антивирустық қорғаныс бағдарламалық жасақтамасы;
- агенттерді қолданатын виртуалды орталарға арналған вирусқа қарсы бағдарламалық құрал;
- бұлтты инфрақұрылымға арналған бағдарламалық жасақтама;
- орталықтандырылған басқару, мониторинг және жаңартудың бағдарламалық құралдары;
- зиянды бағдарламалар мен шабуылдардың жаңартылатын мәліметтер базасы.

2.3 Виртуалды ортаны антивирустық қорғаудың агентсіз бағдарламалық құралдарына қойылатын талаптар.

Серверлер үшін келесі операциялық жүйелерді қолдауы керек:

- Windows Server 2022.
- Windows Server 2019.
- Windows Server 2016.
- Windows Server 2012 R2.
- Windows Server 2012.
- Windows Server 2008 R2 жаңарту бумасы 1.

Виртуалды орталарды вирусқа қарсы қорғаудың бағдарламалық құралдары мынадай функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс:

- қонақ машиналарына антивирустық агент орнатпай нақты уақыт режимінде және жоспарланған тексеру режимінде зиянды бағдарламадан қорғау;
- өшірулі қонақ машиналарын, зиянды бағдарламалардың бар-жоғын тексеру кезінде оларды қосудың қажеті жоқ сканерлеу, соның ішінде Linux ОЖ бар қонақ машиналары;
- барлық қорғаныс компоненттері үшін бірыңғай басқару консолі;
- виртуалды орталар мен физикалық жұмыс станциялары үшін орталықтандырылған басқару;
- ВМ үлгілерін тексеру;
- қолданбаға нақты уақыт режимінде және жоспарланған тексеру режимінде файл үкімін алу үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау;
- қонақ машиналарына жаңартуларды таратудың қажеті жоқ орталықтандырылған базалық жаңартулар;
- таңдалған файлдарды, қалталарды және бүкіл жүйені сканерлеу;
- тексерілген файлдарды қайта сканерлеуден аулақ болатын сканерлеу режимін оңтайландыру;
- бір гипервизордың ішінде әртүрлі қонақ машиналарында бірдей нысандарды қайта сканерлеудің алдын алу;
- әкімшіні хабардар ете отырып, зиянды бағдарламаны бұғаттау, залалсыздандыру және жою;
- виртуалды машиналардағы оқиғалар және тапсырмаларды орындау туралы толық ақпаратты көрсету;
- виртуалды машиналардың жеке топтары үшін әртүрлі қауіпсіздік параметрлерін қолдану;
- жойылған файлдардың сақтық көшірмелерін сақтау;
- пайдаланушы тіркелгісінің рөліне байланысты саясат пен тапсырма параметрлеріне қол жеткізуді шектеу;
- ең жиі тексерілетін файлдар туралы статистиканы көрсету.

2.4 Агенттерді пайдалана отырып виртуалды орталарды вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар.

Виртуалды Инфрақұрылым:

- Windows Server 2016 Hyper-V;
- Windows Server 2019 Hyper - V және одан жоғары;

Қонақ операциялық жүйелері:

- Windows 10 Enterprise 2019 LTSC / 19h1 / 19H2 / 20H1 / 20H2 / 21h1 (32 / 64 биттік) және одан жоғары.
- Windows 8.1 Update 1 professional / Enterprise (32 / 64 биттік).
- Windows 7 Professional / Enterprise Service Pack 1 (32 / 64 бит).
- Windows Server 2022 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2019 Standard / Datacenter (Desktop experience / Core).
- Windows Server 2016 Standard / Datacenter (Desktop experience / Core).
- Windows Server 2012 R2 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2012 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (Desktop experience / Core).
- Debian GNU / Linux 10.1 және одан жоғары (32 / 64 бит).
- Debian GNU / Linux 9.4 және одан жоғары (32 / 64 бит).
- Ubuntu Server 20.04 LTS (64 бит).
- Ubuntu Server 18.04 LTS (64 бит).
- CentOS 8.0 және одан жоғары (64 бит).
- CentOS 7.3 және одан жоғары (64 бит).

Виртуалды орталарды вирусқа қарсы қорғаудың бағдарламалық құралдары мынадай функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс:

1) Windows ОЖ жұмыс станцияларында:

- барлық қорғаныс компоненттері үшін бірыңғай басқару консолі;
- резиденттік антивирустық мониторинг;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- антивирустық сканерлеуді және басқа ресурстарды қажет ететін тапсырмаларды қонақ машиналарында емес, жеке қорғаныс машинасында орындау;
- ВМ агенттерін автоматты түрде анықтау және жұмыс істеп тұрған қорғау машинасына қосу, негізгі қорғау машинасы болмаған жағдайда басқа да хосттағы агенттерге қосу;
- қорғау машинасының қол жетімсіздігі кезеңінде қорғалған қонақтар машинасында барлық файлдық операцияларды журналдау арқылы қорғау машинасының қысқа мерзімді қол жетімсіздігі кезеңінде файлдық қорғаудың үздіксіздігін қамтамасыз ету және кіру қалпына келтірілгеннен кейін барлық өзгерістерді автоматты түрде сканерлеуді орындау;
- нақты уақыт режимінде сканерлеу кезінде және жоспарланған тексеру режимінде файл бойынша үкім шығару үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау;
- келесі хаттамаларда трафикті тексере отырып, зиянды бағдарламалардан электрондық хат-хабарларды қорғау: IMAP, SMTP, POP3 – пайдаланылатын электрондық пошта клиентіне қарамастан;
- Outlook клиентіне арналған қосымшаны тексеруді қосу/өшіру, сондай-ақ тіркемені жою немесе кірістірілген файл пішімін өзгерту мүмкіндігі бар электрондық пошта плагині;
- веб-трафикті қорғау-пайдаланушының компьютеріне HTTP, HTTPS, FTP хаттамалары бойынша, оның ішінде эвристикалық талдау арқылы, сенімді сайттарды теңшеу мүмкіндігімен келетін объектілерді тексеру;
- -веб-беттерден жүктелген баннерлер мен қалқымалы терезелерді бұғаттау;
- фишингтік сайттарды тану және бұғаттау;
- олардың мінез-құлқын талдау негізінде әлі белгісіз зиянды бағдарламалардан қорғау;
- осы қолданбаның әрекеттерін талдау арқылы қолданбаның қалыптан тыс әрекетін анықтау мүмкіндігі;
- емдеу кезінде зиянды бағдарламалық қамтамасыз ету әрекеттерін кері қайтару мүмкіндігі;
- ортақ файлдар мен қалталарды сыртқы шифрлаудан қорғау;
- тізілімге жазу, Файлдар мен қалталарға кіру сияқты орындалатын бағдарламалардың артықшылықтарын шектеу мүмкіндігі. Бағдарламаның беделіне негізделген шектеу деңгейлерін автоматты түрде анықтау;
- барлық немесе белгілі бір пайдаланушы топтары (AD немесе жергілікті пайдаланушылар/топтар)үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелер жасауға мүмкіндік беретін компоненттің болуы;
- арнайы ережелерді құру компоненті бағдарламаны, метадеректерді, сертификатты немесе оның ізін, MD5 немесе SHA256 бақылау сомасын табу жолында қосымшаларды бақылауы керек;
- арнайы ережелерді құру компоненті қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе бұғаттау режимінде жұмыс істеуі керек, оларға салынған файлдарды өзгерте және іске қоса алатын сенімді жаңарту пакеттерінің тізімін жасай алуы керек;
- белгілі бір протоколдар (TCP, UDP) және порттар үшін желілік пакеттік ережелерді орнатуға және белгілі бір бағдарламалар үшін желілік ережелерді құруға мүмкіндік беретін кіріктірілген желілік экранның болуы;
- кез-келген типтегі есептеу желілерінде, соның ішінде сымсыз желілерде жұмыс істеу кезінде ең танымал қосымшаларға арналған интрузияны анықтау және алдын-алу жүйесі (IDS/IPS) және желілік белсенділік ережелері бар брандмауэр арқылы хакерлік шабуылдардан қорғау;
- құрылғының типі және/немесе пайдаланылатын Шина бойынша сыртқы енгізу/шығару құрылғыларымен пайдаланушының жұмысын бақылауды жүзеге асыру, олардың идентификаторы бойынша сенімді құрылғылардың тізімін жасау мүмкіндігі және ad ішінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігі;
- пайдаланушының Интернет желісімен жұмысын бақылауды жүзеге асыру, оның ішінде белгілі бір сипаттағы ресурстарға қол жеткізуге нақты тыйым салу немесе рұқсат беру, сондай-ақ ақпараттың белгілі бір түрін (аудио, видео және т.б.) бұғаттау мүмкіндігі.
- бағдарламалық құрал бақылаудың уақыт аралықтарын енгізуге мүмкіндік беруі керек, сонымен қатар оны тек AD ішінен белгілі бір пайдаланушыларға тағайындауы керек;
- барлық виртуалды машиналарды алдын-ала белгіленген кесте бойынша тексеру мүмкіндігі.
- тексерілген файлдарды қайта қарап шығудың алдын алу;
- әр түрлі виртуалды машиналарда орналасқан бірдей файлдарды қайта тексеруді болдырмауға мүмкіндік беретін қорғау машинасында тексерілген файлдар туралы ақпараттың болуы;
- зиянды бағдарламаны бұғаттау, залалсыздандыру және жою, әкімшілерге хабарлау;
- виртуалды машиналардың жеке топтары үшін әртүрлі қауіпсіздік параметрлерін қолдану мүмкіндігі;
- жойылған файлдардың сақтық көшірмелерін сақтау;
- антивирустық базаларды кері қайтаруды қолдау;
- қолдану аясын одан әрі шектеуге мүмкіндік беретін антивирустық параметрлерді профильдеу механизмі.

2) Windows серверлік операциялық жүйелерінде:

- барлық қорғаныс компоненттері үшін бірыңғай басқару консолі;
- резиденттік антивирустық мониторинг.
- маскировка бағдарламаларынан, ақылы сайттарға автоматты түрде қоңырау шалу бағдарламаларынан қорғау.
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор.
- антивирустық сканерлеуді және басқа ресурстарды қажет ететін тапсырмаларды қонақ машиналарында емес, жеке қорғаныс машинасында орындау;
- келесі хаттамалардағы трафикті тексере отырып, зиянды бағдарламалардан электрондық хат-хабарларды қорғау: IMAP, SMTP, POP3 — пайдаланылатын электрондық пошта клиентіне қарамастан.
- негізгі қорғаныс машинасы болмаған жағдайда, жұмыс істеп тұрған қорғаныс машинасын, оның ішінде басқа хостта орналасқан машинаны автоматты түрде анықтау және қосу.
- қорғау машинасының қолжетімсіздігі кезеңінде қорғалған қонақ машинасында барлық файлдық операцияларды журналдау арқылы қорғау машинасының қысқа мерзімді қол жетімсіздігі кезеңінде файлдық қорғаудың үздіксіздігін қамтамасыз ету және кіру қалпына келтірілгеннен кейін барлық өзгерістерді автоматты түрде сканерлеуді орындау.
- нақты уақыт режимінде сканерлеу кезінде және жоспарланған тексеру режимінде файл бойынша үкім шығару үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау.
- олардың мінез-құлқын талдау негізінде әлі белгісіз зиянды бағдарламалардан қорғау.
- ортақ файлдар мен қалталарды сыртқы шифрлаудан қорғау;
- белгілі бір протоколдар (TCP, UDP) және порттар үшін желілік пакеттік ережелерді орнатуға мүмкіндік беретін кіріктірілген желі экранының болуы.
- нақты бағдарламаларға арналған желілік ережелерді құру;
- кез-келген типтегі есептеу желілерінде, соның ішінде сымсыз желілерде жұмыс істеу кезінде ең танымал қосымшаларға арналған интрузияны анықтау және алдын-алу жүйесі (IDS/IPS) және желілік белсенділік ережелері бар брандмауэр арқылы хакерлік шабуылдардан қорғау.
- антивирустық базалардың бір бөлігін қорғау машинасында сақтау мүмкіндігі бар орталықтандырылған жаңартулар;
- барлық виртуалды машиналарды алдын-ала белгіленген кесте бойынша тексеру мүмкіндігі.
- тексерілген файлдарды қайта қарап шығудың алдын алу.
- әр түрлі виртуалды машиналарда орналасқан бірдей файлдарды қайта тексеруді болдырмауға мүмкіндік беретін қорғаныс машинасында тексерілген файлдар туралы ақпараттың болуы.
- зиянды бағдарламаны бұғаттау, залалсыздандыру және жою, әкімшілерге хабарлау.
- виртуалды орталар мен физикалық жұмыс станциялары үшін бірыңғай орталықтандырылған басқару консолі.
- виртуалды машиналардағы оқиғалар және тапсырмаларды орындау туралы толық ақпарат беру.
- виртуалды машиналардың жеке топтары үшін әртүрлі қауіпсіздік параметрлерін қолдану мүмкіндігі.
- жойылған файлдардың сақтық көшірмелерін сақтау.
- антивирустық базаны кері қайтаруды қолдау.
- қолдану аясын одан әрі шектеуге мүмкіндік беретін антивирустық параметрлерді профильдеу механизмі.

3) Linux серверлік операциялық жүйелерінде:

- бірыңғай басқару жүйесін қолдана отырып, жоғарыда аталған барлық компоненттерді орталықтандырылған басқару.
- резиденттік антивирустық мониторинг;
- бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу;
- zip мұрағаттарындағы файлдарды антивирустық тексеру; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
- электрондық пошта хабарламаларын мәтіндік форматта тексеру (Plain text);
- файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытының шегі, тексерілетін файл өлшемінің шегі, кэштеу механизмі тексерілген және тексерілгеннен кейін өзгертілмеген файлдар туралы ақпарат);
- күдікті және бүлінген объектілерді карантинге орналастыру;
- тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосыңыз;
- есептерді HTML және CSV форматтарында экспорттау және сақтау мүмкіндігі;
- егер ол ақпараттық құндылықты білдірсе, талап бойынша Объектіні ықтимал қалпына келтіру мақсатында емдеу және жою алдында залалданған объектінің көшірмесін резервтік қоймада сақтау;
- жүктеу секторларын, жүйелік жадты және автоматты іске қосу объектілерін тексеру мүмкіндігі.

2.5 Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдарына қойылатын талаптар.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек:

- виртуалды орталар мен физикалық жұмыс станциялары үшін бірыңғай орталықтандырылған басқару консолі.
- қорғалатын тораптардың санына байланысты орталықтандырылған басқару, мониторинг және жаңарту құралын орнату архитектурасын таңдау;
- ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында AD-дан ақпаратты оқу мүмкіндігі;
- анықталған компьютерлерді IP-мекен-жайға, ОЖ түріне, OU AD-да болу ережелерін теңшеу мүмкіндігі;
- желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтары бойынша автоматты түрде бөлу;
- IP мекенжайы, ОЖ типі, OU AD-да болу бойынша тасымалдау ережелерін теңшеу мүмкіндігі;
- орталықтандырылған антивирустық қорғаныс бағдарламалық жасақтамасын орнату, жаңарту және жою;
- орталықтандырылған орнату, әкімшілік;
- қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау;
- басқару орталығының құралдарымен үйлеспейтін қосымшаларды орталықтандырылған жою (қолмен және автоматты) ;
- саясат пен міндеттердің өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;
- антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін-RPC, GPO, басқару жүйесінің құралдары, жергілікті орнату үшін-дербес орнату пакетін құру мүмкіндігі;
- қауіпсіздік саясатында пайдаланушы кірген есептік жазбаға, ағымдағы IPv4 мекенжайына, сондай-ақ компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты антивирустық шешімнің параметрлерін қайта анықтайтын арнайы триггерлерді көрсету мүмкіндігі;
- қайта бөлу орын алатын триггерлер иерархиясының мүмкіндігі;
- клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу;
- жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
- виртуалды машиналар желісінде тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу;
- әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігімен көп деңгейлі басқару жүйесін құру;
- еркін деңгейдегі басқару серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
- әкімшілік сервер иерархиясында шифрлауды басқару мүмкіндігі;
- басқару серверлеріне арналған multi-tenancy қолдауы;
- -оқшауланған виртуалды инфрақұрылымдарды қорғау үшін провайдер сервисі инфрақұрылымында multi-tenancy режимін қолдау;
- байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту;
- басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қол жеткізу;
- клиенттік компьютерлерге лицензияны автоматты түрде тарату;
- пайдаланушылардың компьютерлерінде орнатылған БҚ мен жабдықты түгендеу;
- орнатылған антивирустық қорғау Қосымшаларының жұмысындағы оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді баптау;
- Exchange ActiveSync сервері арқылы мобильді құрылғыларды басқару функциясы;
- iOS MDM сервері арқылы мобильді құрылғыларды басқару мүмкіндігі;
- берілген оқиғалар туралы SMS-хабарламаларды жіберу мүмкіндігі;
- басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату;
- басқару жүйесіне желілік жүктемені азайту үшін кез-келген компьютерді ұйымның жаңартуларды қайта жіберу орталығымен көрсету мүмкіндігі;
- кез-келген компьютерді ұйымға антивирустық агенттердің оқиғаларын жіберу орталығы, клиенттік компьютерлердің таңдалған тобы, басқару жүйесіне желілік жүктемені азайту үшін орталықтандырылған басқару сервері ретінде көрсету мүмкіндігі;
- виртуалды машиналарда орнатылған қосымшаларда және операциялық жүйеде осалдықтарды іздеу бойынша тапсырманың болуы;
- вирусқа қарсы қорғау оқиғалары, түгендеу деректері, белгіленген бағдарламаларды лицензиялау деректері бойынша графикалық есептерді құру;
- жүйенің жұмысы туралы алдын ала конфигурацияланған стандартты есептердің болуы;
- есептерді PDF және XML форматындағы файлдарға экспорттау;
- syslog хаттамасы бойынша оқиғаларды сыртқы жүйелерге экспорттау;

- антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин объектілерін орталықтандырылған басқару;
- басқару серверінде аутентификация үшін ішкі есептік жазбаларды құру;
- басқару жүйесінің кіріктірілген құралдарын басқару жүйесінің резервтік көшірмесін жасау;
- Windows Failover Clustering қолдауы;
- Certificate Authority қызметімен Windows интеграциясын қолдау;
- пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы;
- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- Microsoft Azure және Google Cloud бұлтты инфрақұрылымында орнату мүмкіндігі;
- OpenApi интеграциялау мүмкіндігі;
- Web консолін пайдаланып антивирустық қорғауды басқару мүмкіндігі.
- әкімшілік консоліне рұқсатсыз кіру қаупін азайту үшін екі сатылы тексеруді орнату мүмкіндігі;
- қосымша пайдалану аутентификация пайдаланушы тіркелгісінің параметрлерін өзгерткеннен кейін.
- IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрау мүмкіндігі;
- қол жетімділігі жоғары жүйе ретінде әкімшілік серверді орналастыру мүмкіндігі.

3. Қызмет көрсету шарттары.

Қорғалатын виртуалды машиналар саны немесе процессорлар саны бойынша лицензиялау схемасын қолдау.

Лицензияланған антивирустық қорғаныс өнімдері үнемі жаңартылып отыруға міндетті. Жаңартылатын антивирустық мәліметтер базасы келесі функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс:

- күнтізбелік тәулік ішінде кемінде 24 рет антивирустық базаларды жаңарту қағидаларын құру ережесі;
- жаңарту жолдарының көптігі, оның ішінде-әртүрлі байланыс арналары мен портативті электрондық ақпарат тасымалдағыштар арқылы;
- электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру.

Лицензияланған антивирустық қорғаныс өнімдері бағдарламалық жасақтама өндірушісінен техникалық қызмет көрсетуді қамтуы керек. Техникалық қызмет көрсету өндірушіден тәулік бойы қолдау көрсету құқығын қамтамасыз етуі керек және олар пайда болған сайын өнімді және оның барлық компоненттерін әр жаңа нұсқамен жаңартуы керек. Антивирустық шешім өндірушісінің веб-сайтында антивирустық шешімді техникалық қолдауға арналған арнайы бөлім, жаңартылатын білім базасы, сондай-ақ бағдарламалық өнімдерді пайдаланушылар форумы болуы керек.

4. Қызмет көлемі.

Орындаушы 01.01.2025ж. бастап 31.12.2025ж. дейін әрекет ететін 70 бірлік виртуалды серверлер үшін вирусқа қарсы қорғау құралдарына лицензия беру арқылы осы техникалық сипаттамаға сәйкес қызметтер көрсетуге міндеттенеді.

Қол қойған	ШЫНЫБАЕВ БАТЫРБЕК ЖАНИБЕКОВИЧ
Қол қойылған күні	20.09.2024

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1031888
способом Запрос ценовых предложений

Лот № 5 (18 У, 3765662) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Акционерное общество "Каражанбасмунай"

Организатор: Акционерное общество "Каражанбасмунай"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	18 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	Услуги по предоставлению подписки на систему защиты виртуальных серверов
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, Мангистауская область, Актау Г.А., г.Актау, мкр.9 А, БЦ Елес
Условия поставки	-
Срок поставки	с 01.2025 по 03.2025 (включительно)
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

2.1 Термины, сокращения и определения:

Услуги – Услуги по предоставлению подписки на систему защиты виртуальных серверов;

ОС – Операционная система;

Виртуальная машина, ВМ – это виртуальный компьютер, работающий как настоящий компьютер внутри виртуальной среды. Выражаясь проще, это приложение, которое имитирует компьютер с полноценной операционной системой и аппаратным обеспечением;

Виртуальный сервер – это сервер, функционирующий на базе виртуальной машины;

ПО – программное обеспечение;

AD – Active Directory.

2.2 Общие требования.

Антивирусные средства защиты для виртуальных серверов должны защищать виртуальные машины и серверы на базе ОС Windows и Linux. Решение должно включать:

- безагентные программные средства антивирусной защиты для виртуальных сред;
- программные средства антивирусной защиты для виртуальных сред с использованием агентов;
- программные средства защиты для облачной инфраструктуры;
- программные средства централизованного управления, мониторинга и обновления;
- обновляемые базы данных сигнатур вредоносных программ и атак.

2.3 Требования к безагентным программным средствам антивирусной защиты виртуальных сред.

Должна поддерживать следующие операционные системы для серверов:

- Windows Server 2022.
- Windows Server 2019.
- Windows Server 2016.
- Windows Server 2012 R2.
- Windows Server 2012.
- Windows Server 2008 R2 SP1.

Программные средства антивирусной защиты виртуальных сред должны обеспечивать реализацию следующих функциональных возможностей:

- защита от вредоносного ПО в режиме реального времени и в режиме запланированной проверки без установки антивирусного агента на гостевые машины;
- сканирование выключенных гостевых машин, на наличие вредоносного ПО, без необходимости включать их на время проверки, в том числе и гостевые машины с ОС Linux;
- единая консоль управления для всех компонентов защиты;
- централизованное управление для виртуальных сред и физических рабочих станций;
- проверка шаблонов виртуальных машин;
- облачная защита от новых угроз, позволяющая приложению при сканировании в режиме реального времени и в режиме запланированной проверки обращаться к специальным ресурсам производителя, для получения вердикта по файлу;
- централизованные обновления баз без необходимости распространения обновлений на гостевые машины;
- сканирование выбранных файлов, папок и всей системы;
- оптимизация режима сканирования, которая позволяет избегать повторного сканирования уже проверенных файлов;
- предотвращение повторного сканирования одинаковых объектов на разных гостевых машинах рамках одного гипервизора;
- блокирование, обезвреживание и удаление вредоносного ПО с уведомлением администраторов;
- отображение подробной информации о событиях на виртуальных машинах и о выполнении задач;
- применение различных параметров безопасности для отдельных групп виртуальных машин;
- хранение резервных копий удаленных файлов;
- разграничение доступа к параметрам политик и задач в зависимости от роли учетной записи пользователя;
- отображение статистики о наиболее часто проверяемых файлах.

2.4 Требования к программным средствам антивирусной защиты виртуальных сред с использованием агентов.

Виртуальная инфраструктура:

- Windows Server 2016 Hyper-V;
- Windows Server 2019 Hyper-V и выше;

Гостевые операционные системы:

- Windows 10 Enterprise 2019 LTSC / 19H1 / 19H2 / 20H1 / 20H2 / 21H1 (32 / 64-разрядная) и выше.
- Windows 8.1 Update 1 Professional / Enterprise (32 / 64-разрядная).
- Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-разрядная).
- Windows Server 2022 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2019 Standard / Datacenter (Desktop experience / Core).
- Windows Server 2016 Standard / Datacenter (Desktop experience / Core).
- Windows Server 2012 R2 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2012 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (Desktop experience / Core).– —
- Debian GNU / Linux 10.1 и выше (32 / 64-разрядная).
- Debian GNU / Linux 9.4 и выше (32 / 64-разрядная).
- Ubuntu Server 20.04 LTS (64-разрядная).
- Ubuntu Server 18.04 LTS (64-разрядная).
- CentOS 8.0 и выше (64-разрядная).
- CentOS 7.3 и выше (64-разрядная).

Программные средства антивирусной защиты виртуальных сред должны обеспечивать реализацию следующих функциональных возможностей:

1) На рабочих станциях ОС Windows:

- единая консоль управления для всех компонентов защиты;
- резидентный антивирусный мониторинг;
- эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
- выполнение антивирусного сканирования и других ресурсоемких задач не на гостевых машинах, а на отдельной машине защиты;
- автоматическое обнаружение и подключение агентов на ВМ к функционирующей машине защиты, в том числе находящейся на другом хосте, в случае недоступности основной машины защиты;
- обеспечение непрерывности файловой защиты в период кратковременной недоступности машины защиты посредством журналирования всех файловых операций на защищаемой гостевой машине в период недоступности машины защиты, и выполнение автоматического сканирования всех изменений после восстановления доступа;
- облачная защита от новых угроз, позволяющая приложению при сканировании в режиме реального времени и в режиме запланированной проверки обращаться к специальным ресурсам производителя, для получения вердикта по файлу;
- защита электронной корреспонденции от вредоносных программ с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 – независимо от используемого почтового клиента;
- почтовый плагин для клиента Outlook с возможностью включения/отключения проверки вложений, а также возможностью удаления вложения или изменения формата вложенного файла;
- защита веб-трафика – проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных сайтов;
- блокировка баннеров и всплывающих окон, загружаемых с Web-страниц;
- распознавание и блокировка фишинг-сайтов;
- защита от еще не известных вредоносных программ на основе анализа их поведения;
- возможность определения аномального поведения приложения с помощью анализа действий этого приложения;
- возможность совершить откат действий вредоносного программного обеспечения при лечении;
- защита от внешнего шифрования общих файлов и папок;
- возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы;
- наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (AD или локальных пользователей/групп);
- компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256;
- компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должен иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
- наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов, а также создание сетевых правил для конкретных программ;
- защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
- осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из AD;
- осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.).
- программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из AD;
- возможность проверки всех виртуальных машин по заранее заданному расписанию.
- предотвращение повторного сканирования уже проверенных файлов;
- наличие информации о проверенных файлах на машине защиты, позволяющей исключить повторную проверку одних и тех же файлов, находящихся на разных виртуальных машинах;
- блокирование, обезвреживание и удаление вредоносного ПО, уведомление администраторов;
- возможность применять различные параметры безопасности для отдельных групп виртуальных машин;
- хранение резервных копий удаленных файлов;

- поддержка отката антивирусных баз;
- механизм профилирования настроек антивируса, позволяющий дополнительно ограничить область ее применения.

2) На серверных операционных системах Windows:

- единая консоль управления для всех компонентов защиты
- резидентный антивирусный мониторинг.
- защита от программ-маскировщиков, программ автодозвона на платные сайты.
- эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.
- выполнение антивирусного сканирования и других ресурсоемких задач не на гостевых машинах, а на отдельной машине защиты;
- защита электронной корреспонденции от вредоносных программ с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента.
- автоматическое обнаружение и подключение к функционирующей машине защиты, в том числе находящейся на другом хосте, в случае недоступности основной машины защиты.
- обеспечение непрерывности файловой защиты в период кратковременной недоступности машины защиты посредством журналирования всех файловых операций на защищаемой гостевой машине в период недоступности машины защиты, и выполнение автоматического сканирования всех изменений после восстановления доступа.
- облачная защита от новых угроз, позволяющая приложению при сканировании в режиме реального времени и в режиме запланированной проверки обращаться к специальным ресурсам производителя, для получения вердикта по файлу.
- защита от еще не известных вредоносных программ на основе анализа их поведения.
- защита от внешнего шифрования общих файлов и папок;
- наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов.
- создание сетевых правил для конкретных программ;
- защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные.
- централизованные обновления с возможностью хранения части антивирусных баз на машине защиты;
- возможность проверки всех виртуальных машин по заранее заданному расписанию.
- предотвращение повторного сканирования уже проверенных файлов.
- наличие информации о проверенных файлах на машине защиты, позволяющей исключить повторную проверку одних и тех же файлов, находящихся на разных виртуальных машинах.
- блокирование, обезвреживание и удаление вредоносного ПО, уведомление администраторов.
- консоль централизованного управления, единая для виртуальных сред и физических рабочих станций.
- предоставление подробной информации о событиях на виртуальных машинах и о выполнении задач.
- возможность применять различные параметры безопасности для отдельных групп виртуальных машин.
- хранение резервных копий удаленных файлов.
- поддержка отката антивирусных баз.
- механизм профилирования настроек антивируса, позволяющий дополнительно ограничить область ее применения.

3) На серверных операционных системах Linux:

- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
- резидентный антивирусный мониторинг;
- эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
- проверка сообщений электронной почты в текстовом формате (Plain text);
- наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
- помещение подозрительных и поврежденных объектов на карантин;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
- сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
- возможность проверки загрузочных секторов, системной памяти и объектов автозапуска.

2.5 Требования к программным средствам централизованного управления, мониторинга и обновления.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- консоль централизованного управления, единая для виртуальных сред и физических рабочих станций.
- выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
- возможность чтения информации из AD, с целью получения данных об учетных записях компьютеров и пользователей в организации;
- возможность настройки правил переноса обнаруженных компьютеров по IP-адресу, типу ОС, нахождению в OU AD;
- автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети;
- возможность настройки правил переноса по IP-адресу, типу ОС, нахождению в OU AD;
- централизованные установка, обновление и удаление программных средств антивирусной защиты;
- централизованная настройка, администрирование;
- просмотр отчетов и статистической информации по работе средств защиты;
- централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
- сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
- наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
- возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
- возможность иерархии триггеров, по которым происходит перераспределение;
- тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
- доставка обновлений на рабочие места пользователей сразу после их получения;
- распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
- построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
- возможность управления шифрованием в иерархии серверов администрирования;
- поддержка multi-tenancy для серверов управления;
- поддержка режима multi-tenancy в инфраструктуре сервис провайдера для защиты изолированных виртуальных инфраструктур;
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
- доступ к облачным серверам производителя антивирусного ПО через сервер управления;
- автоматическое распространение лицензии на клиентские компьютеры;
- инвентаризация установленного ПО и оборудования на компьютерах пользователей;
- наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
- функция управления мобильными устройствами через сервер Exchange ActiveSync;
- функция управления мобильными устройствами через сервер iOS MDM;
- возможность отправки SMS-оповещений о заданных событиях;
- централизованная установка сертификатов на управляемые мобильные устройства;
- возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
- возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
- наличие задачи по поиску уязвимостей в установленных приложениях и операционной системе на виртуальных машинах;
- построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
- наличие преднастроенных стандартных отчетов о работе системы;
- экспорт отчетов в файлы форматов PDF и XML;
- экспорт событий во внешние системы по протоколу Syslog;

- централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
- создание внутренних учетных записей для аутентификации на сервере управления;
- создание резервной копии системы управления встроенными средствами системы управления;
- поддержка Windows Failover Clustering;
- поддержка интеграции с Windows сервисом Certificate Authority;
- наличие портала самообслуживания пользователей;
- наличие системы контроля возникновения вирусных эпидемий;
- возможность установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
- возможность интеграции по OpenAPI;
- возможность управления антивирусной защитой с использованием WEB консоли.
- возможность настройки двухэтапной проверки для снижения риска несанкционированного доступа к Консоли администрирования;
- использования дополнительной аутентификация после изменения параметров учетной записи пользователя.
- возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами;
- возможность развернуть сервер администрирования как систему высокой доступности.

3. Условия оказания услуг.

Поддержка схемы лицензирования по числу защищаемых виртуальных машин или по количеству процессоров.

Лицензионные продукты антивирусной защиты обязаны обновляться на постоянной основе. Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;
- множественность путей обновления, в том числе – по различным каналам связи и на переносных электронных носителях информации;
- проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Лицензионные продукты антивирусной защиты обязаны включать техническое обслуживание от производителя программного обеспечения. Техническое обслуживание должно предоставлять право на круглосуточную поддержку от производителя и обновлять продукт и все его компоненты с каждой новой версией по мере их появления. Web-сайт производителя антивирусного решения должен иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

1. **Объемы услуг**

Исполнитель обязуется оказать Услуги согласно с настоящей технической спецификацией путем предоставления лицензии на средства антивирусной защиты для виртуальных серверов в количестве 70 единиц, действующих с 01.01.2025г. по 31.12.2025г.

Подписал	ШЫНЫБАЕВ БАТЫРБЕК ЖАНИБЕКОВИЧ
Дата подписания	20.09.2024