ТЕХНИКАЛЫҚ СИПАТТАМА

1027681 сатып алу бойынша
Төмендету баға ұсыныстарын сұрату тәсілімен

Лот № 1 (116-1 У, 3753579) Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер

Тапсырыс беруші: "QazCloud (КазКлауд)" Жауапкершілігі шектеулі серіктестігі

Ұйымдастырушы: "QazCloud (КазКлауд)" Жауапкершілігі шектеулі серіктестігі

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	116-1 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер, Бағдарламалық қымсыздандыруды пайдалану құқығына лицензияны создыру бойынша қызметтер
Қосымша сипаттама	-
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., пр.Мангилик ел 35А
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 15 күнтізбелік күні
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

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

I БӨЛІМ. ТЕХНИКАЛЫҚ ТАПСЫРМА

Лицензияланған бағдарламалық жасақтаманы (антивирус) пайдалану құқығын ұзарту жөніндегі қызмет

Лицензиялық бағдарламалық жасақтаманы (бұдан әрі - БЖ) пайдалану құқығын ұзарту жөніндегі қызмет Тапсырыс берушінің электрондық мекенжайына электрондық түрде ұсынылуы тиіс.

1. **ҰСЫНЫЛАТЫН ҚЫЗМЕТТІҢ СИПАТЫ ЖӘНЕ ТАЛАП ЕТІЛЕТІН**

ТЕХНИКАЛЫҚ, САПАЛЫҚ ЖӘНЕ ПАЙДАЛАНУ СИПАТТАМАЛАРЫ.

Лицензиялық бағдарламалық жасақтаманы пайдалану құқығын ұзарту жөніндегі қызмет (антивирус) лицензиялық БЖ-ны біржолғы төлем шартымен №1 кестеге сәйкес (бағдарламалық жасақтаманы қолдануға айрықша емес құқықтарды беру) қолдануды көздейді.

Лицензияланған бағдарламалық жасақтаманың атаулары (антивирус): Kaspersky Endpoint Security for Business - Select Kazakhstan Edition. 10–14 Node 1 year Base License.

Жалпы талаптар

Антивирустық құралдар келесілерден құралуы тиіс:

Windows жұмыс станциялары мен серверлеріне арналған антивирустық қорғаныс бағдарламалық құралдары;

Linux жұмыс станциялары мен серверлеріне арналған антивирустық қорғаныс бағдарламалық құралдары;

орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары;

зиянды бағдарламалар мен шабуылдар сигнатураларының жаңартылатын дерекқорлары;

орыс тіліндегі пайдалану құжаттамасы.

Барлық антивирустық құралдардың, соның ішінде басқару құралдарының бағдарламалық интерфейсі орыс және ағылшын тілдерінде болуы керек.

Барлық антивирустық құралдарының, соның ішінде басқару элементтерінің орыс және ағылшын тілдерінде контексті анықтамалық жүйесі болуы керек.

Windows жұмыс станцияларына арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар

Антивирустық қорғаныс бағдарламалық жасақтамасы келесі нұсқалардағы жұмыс станцияларына арналған операциялық жүйені басқаратын компьютерлерде жұмыс істеуі керек:

o Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 және одан жоғары;

o Windows 8 Professional / Enterprise (32 / 64-разрядты);

o Windows 8.1 Professional / Enterprise (32 / 64-разрядты);

o Education / Enterprise жұмыс станцияларына арналған Windows 10 Home / Pro / Pro;

o Education / Enterprise жұмыс станцияларына арналған Windows 11 Home / Pro / Pro.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер жүзеге асырылуы тиіс:

- нақты уақыт режимінде және нысанның контекстік мәзірінен сұраныс бойынша
- антивирустық сканерлеу; кесте бойынша антивирустық сканерлеу;
- қосылатын құрылғыларды антивирустық сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық талдауыштар;
- белсенді зақымдану әрекеттерін бейтараптандыру;
- қолданбаның мінез-құлқын және оның зиянды белсенділігін және рұқсат етілмеген әрекеттерді анықтау үшін жүйеде жасаған әрекеттерін талдау;
- желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ папкалар мен файлдарға жүгінуін талдау;
- бағдарламалық жасақтамадағы осалдықтарын пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау оның ішінде жүйелік үрдістерінің жадын қорғау;
- сауықтыру кезінде зиянды бағдарламалық жасақтама әрекеттерін кері қайтару, оның ішінде шифрланған, зиянды бағдарламалармен, файлдармен қалпына келтіру;
- үрдістер мен қосымшаларға арналған артықшылық шектеулері (тізілімге жазылу, файлдарға, папкаларға және басқа үрдістерге қол жеткізу, тапсырмаларды жоспарлаушыға хабарласу, құрылғыларға қол жеткізу, нысандарға құқықтарды өзгерту және т. б.) сенім деңгейін анықтай отырып, динамикалық түрде жаңартылатын күйге келтірілетін қолданбалар тізімдері;
- іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау;

- келесі форматтағы мұрағаттардағы файлдарды антивирустық тексеру және сауықтыру: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- IMAP, SMTP, POP3, MAPI, NNTP хаттамалары арқылы берілетін кіріс және

шығыс трафикті тексерумен электрондық поштаны зиянды бағдарламалардан қорғау;

- берілген файл түрлерінің атын өзгерту немесе жою мүмкіндігі бар пошта тіркемелерінің сүзгісі;
- HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP хаттамалары бойынша пайдаланушының компьютеріне келіп түсетін желілік трафикті, оның ішінде эвристикалық талдау, сенімді ресурстарды күйге келтіру мүмкіндігі және құлыптау немесе статистика режимінде жұмыс істеу арқылы тексеру;
- жүктелетін Web -беттердегі баннерлер мен қалқымалы терезелерді бұғаттау;
- фишингтік және қауіпті сайттарды тану және бұғаттау;
- желілік сегменттерді санаттау мүмкіндігі бар бағдарламалар үшін желілік пакеттік ережелер мен желілік ережелерді құруға мүмкіндік беретін бірге құқрылған желі экраны;
- кез-келген үлгідегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран ережелерін қолдана отырып, желілік шабуылдардан қорғау;
- құрылғының MAC мекенжайын қолдан жасау үшін ARP хаттамасындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
- бірнеше желілік қосылымдарды бір уақытта орнатуды бұғаттау мүмкіндігі бар желілік көпір түріндегі желілік қосылымдарды басқару;
- барлық немесе белгілі бір пайдаланушы топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелер жасау, компонент бағдарламаларды бағдарламаны табу жолында да, метадеректерде, сертификатта немесе оның ізінде, бақылау сомасында және бағдарламалық жасақтаманы өндіруші ұсынған алдын ала белгіленген қолданба санаттарында да бақылауы керек, компонент қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе құлыптау режимінде жұмыс істеуі керек;
- сыртқы енгізу/шығару құрылғыларымен құрылғының түрі және / немесе пайдаланылатын шина бойынша олардың идентификаторы бойынша сенімді құрылғылардың тізімін жасау мүмкіндігімен және Active Directory ішінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігімен пайдаланушының жұмысын бақылау;
- MTP құрылғыларын басқару және құрылғыларды бақылау аясында барлық немесе пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін осы үлгідегі құрылғыларға қол жеткізу ережелерін күйге келтіру;
- алынбалы дискілердегі файлдарды жазу және / немесе жою туралы оқиғалар журналына жазбалар;
- файлдық жүйесі бар құрылғыларға қол жеткізу ережелеріне басымдық беру;
- пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды редакциялауды қосу, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық жаңартылған санатқа, сондай-ақ ақпарат түріне (аудио, бейне және т. б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге мүмкіндік беру, сондай-ақ оны Active Directory-дан тек белгілі бір пайдаланушыларға тағайындау;
- BadUSB үлгісіндегі шабуылдардан қорғау;
- анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтауға арналған арнайы тапсырманы іске қосу;
- қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ құпиясөз арқылы қолданба параметрлеріне кіруді қорғау;
- сенімді қашықтан басқару бағдарламалары арқылы параметрлерді басқару;
- тек таңдалған антивирустық бағдарламалық құрал компоненттерін орнату;
- бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
- тапсырмаларды кесте бойынша және/немесе қолданбаны іске қосқаннан кейін бірден іске қосу;

- файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- өткен тексеру уақытынан бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу үрдісін жеделдету;
- антивирустық бағдарламаның тұтастығын тексеру;
- файлдың бақылау сомасы, аты/директория маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу;
- ережелер мен ерекшеліктер тізімін XML қалыбында импорттау және экспорттау;
- антивируста жойылған вирус жұққан файлдар үшін қорғалған сақтау орны бар, оларды қалпына келтіру мүмкіндігімен;
- антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы;
- антивирустың кескіндік интерфейсін қосу және өшіру, сондай-ақ кескіндік интерфейстің жеңілдетілген нұсқасының болуы, мүмкіндіктердің ең аз жиынтығы;
- Windows Defender Security Center-мен бірігу;
- Antimalware Scan Interface (AMSI) қолдлауының болуы;
- Windows Subsystem for Linux (WSL) қолдауының болуы;
- резервтік қоймадан нысандарды қалпына келтіруді құпия сөзбен қорғау;
- интернет байланысы мөлшерлі болған жағдайда желілік трафиктің шектеулері;
- TCP және UDP хаттамалары бойынша желіні мониторингтеу құралының болуы;
- тексеру үзілген жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;
- тапсырманың орындалу ұзақтығын шектеуді орнату мүмкіндігі;
- тексеру тапсырмаларын кезекке қою мүмкіндігі, егер тексеру қазірдің өзінде орындалса.

Windows серверлеріне арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар

Антивирустық қорғаныстың бағдарламалық құралдары келесі нұсқалардың файлдық

серверлері үшін операциялық жүйені басқаратын компьютерлерде жұмыс істеуі керек:

o Windows Small Business Server 2011 Essentials / Standard (64-разрядты), Microsoft Small Business Server 2011 Standard (64-разрядты) тек орнатылған Service Pack 1 для Microsoft Windows Server 2008 R2; қолдалады;

o Windows MultiPoint Server 2011 (64-разрядты);

o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 және одан жоғары;

o Windows Server 2012 Foundation / Essentials / Standard / Datacenter;

o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;

o Windows Server 2016 Essentials / Standard / Datacenter;

o Windows Server 2019 Essentials / Standard / Datacenter;

o Windows Server 2022.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы т иіс:

- нақты уақыт режимінде және нысанның контекстік мәзірінен сұраныс бойынша

антивирустық сканерлеу; кесте бойынша антивирустық сканерлеу;

- қосылатын құрылғыларды антивирустық сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін

эвристикалық талдауыштар;

- белсенді зақымдану әрекеттерін бейтараптандыру;
- қолданбаның мінез-құлқын және оның зиянды белсенділігін және рұқсат етілмеген әрекеттерді анықтау үшін жүйеде жасаған әрекеттерін талдау;
- желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ папкалар мен файлдарға жүгінуін талдау;
- бағдарламалық жасақтамадағы осалдықтарын пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау оның ішінде жүйелік үрдістердің жадын қорғау;
- сауықтыру кезінде зиянды бағдарламалық жасақтама әрекеттерін кері қайтару, оның ішінде шифрланған, зиянды бағдарламалармен, файлдармен қалпына келтіру;
- іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау;
- келесі форматтағы мұрағаттардағы файлдарды антивирустық тексеру және сауықтыру: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- желілік сегменттерді санаттау мүмкіндігі бар бағдарламалар үшін желілік пакеттік ережелер мен желілік ережелерді құруға мүмкіндік беретін бірге құқрылған желі экраны;
- құрылғының MAC мекенжайын қолдан жасау үшін ARP хаттамасындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
- анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтауға арналған арнайы тапсырманы іске қосу;
- қосымша қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалар, қаскүнемдер немесе біліктілігі жоқ пайдаланушылар тарапынан қорғауды өшірмеуге мүмкіндік беретін құписөз арқылы қолданба параметрлеріне қол жеткізуді қорғау;
- тек таңдалған антивирустық бағдарламалық құрал компоненттерін орнату;
- бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
- тапсырмаларды кесте бойынша және/немесе операциялық жүйені іске қосқаннан кейін бірден іске қосу;
- файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- өткен тексеру уақытынан бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу үрдісін жеделдету;
- антивирустық бағдарламаның тұтастығын тексеру;
- файлдың бақылау сомасы, аты/директория маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу;
- антивируста жойылған вирус жұққан файлдар үшін қорғалған сақтау орны бар, оларды қалпына келтіру мүмкіндігімен;
- антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы;
- антивирустың кескіндік интерфейсін қосу және өшіру, сондай-ақ кескіндік интерфейстің жеңілдетілген нұсқасының болуы, мүмкіндіктердің ең аз жиынтығы;
- Windows Defender Security Center-бірігу;
- Antimalware Scan Interface (AMSI) қолдауының болуы;
- Windows Subsystem for Linux (WSL) қолдауының болуы;
- резервтік қоймадан нысандарды қалпына келтіруді құпия сөзбен қорғау;
- XML-қалыбындағы ережелер мен ерекшеліктер тізімін импорттау және экспорттау;
- интернет байланысы мөлшерлі болған жағдайда желілік трафиктің шектеулері;
- тексеру үзілген жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;
- тапсырманың орындалу ұзақтығын шектеуді орнату мүмкіндігі;

- тексеру тапсырмаларын кезекке қою мүмкіндігі, егер тексеру қазірдің өзінде орындалса.

Linux жұмыс станциялары мен серверлеріне арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар

Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың 32 биттік операциялық жүйелері басқаратын компьютерлерде жұмыс істеуі керек:

o CentOS 6.7 және одан жоғары.

o Debian GNU/Linux 10.1 және одан жоғары.

o Debian GNU/Linux 11.

o Mageia 4.

o Red Hat Enterprise Linux 6.7 және одан жоғары.

o Альт 8 СП Жұмыс Станциясы.

o Альт 8 СП Сервер.

o Альт Білім беру 10.

o Альт Жұмыс Станциясы 10.

Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың 64 биттік операциялық жүйелерімен басқарылатын компьютерлерде жұмыс істеуі тиіс:

o AlmaLinux OS 8 және одан жоғары.

o AlmaLinux OS 9 және одан жоғары.

o AlterOS 7.5 және одан жоғары.

o Amazon Linux 2.

o Astra Linux Common Edition 2.12.

o Astra Linux Special Edition РУСБ.10015-01 (1.5 кезекті жаңарту).

o Astra Linux Special Edition РУСБ.10015-01 (1.6 кезекті жаңарту).

o Astra Linux Special Edition РУСБ.10015-01 (1.7 кезекті жаңарту).

o Astra Linux Special Edition РУСБ.10015-16 (1-орындау) (1.6 кезекті жаңарту).

o CentOS 6.7 және одан жоғары.

o CentOS 7.2 және одан жоғары.

o CentOS Stream 9.

o Debian GNU/Linux 10.1 және одан жоғары.

o Debian GNU/Linux 11.

o EMIAS 1.0.

o EulerOS 2.0 SP5.

o LinuxMint 19.2 және одан жоғары.

o LinuxMint 20.3 және одан жоғары.

o openSUSE Leap 15.0 және одан жоғары.

o Oracle Linux 7.3 жәнеодан жоғары.

o Oracle Linux 8.0 және одан жоғары.

o Red Hat Enterprise Linux 6.7 және одан жоғары.

o Red Hat Enterprise Linux 7.2 және одан жоғары.

o Red Hat Enterprise Linux 8.0 және одан жоғары.

o Red Hat Enterprise Linux 9.

o Rocky Linux 8.5 және одан жоғары.

o SUSE Linux Enterprise Server 12.5 және одан жоғары.

o SUSE Linux Enterprise Server 15 и выше.

o Ubuntu 20.04 LTS.

o Ubuntu 22.04 LTS.

o Альт 8 СП Жұмыс Станциясы.

o Альт 8 СП Сервер.

o Альт Білім беру 10.

o Альт Жұмыс Станциясы 10.

o Альт Сервер 10.

o Атлант, сборка Alcyone, 2022.02. нұсқа.

o Гослинукс 7.17.

o Гослинукс 7.2.

o РЕД ОС 7.3.

o РОСА "Кобальт" 7.9.

o РОСА "Хром" 12.

o ОСОН "ОСНова".

ARM архитектурасына арналған қолдалатын 64-битті операциялық жүйелер:

o Astra Linux Special Edition РУСБ.10152-02 (4.7 кезекті жаңарту).

o EulerOS 2.0 SP8.

o SUSE Linux Enterprise Server 15 SP3.

o Ubuntu 20.04 LTS.

o Альт 8 СП Сервер.

o РЕД ОС 7.3.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы к ерек:

- резидентті антивирустық мониторингтің;
- жаңа қауіптерден бұлтты қорғау, бұл нақты уақыт режимінде бағдарламаның немесе

файлдың үкімін алу үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік береді;

- SMB / NFS арқылы қолжетімді ресурстарды тексеру;
- ядро жадын тексеру мүмкіндігі;
- бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және бұғаттауға мүмкіндік

беретін эвристикалық талдауыш;

- пайдаланушының немесе әкімшінің командасы 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 қалыпта тексеру (Plain text);
- файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді үдерістер, тексеру уақытының шегі, тексерілетін файл өлшемінің шегі, кэштеу механизмі тексерілген және тексерілгеннен кейін өзгертілмеген файлдар туралы ақпарат);
- SMB / NFS хаттамалары бойынша желіге қолжетімді жергілікті каталогтардағы файлдарды қашықтан зиянды шифрлаудан қорғау;
- тексеру кезінде файлдарды бұғаттау опциясын қосу;
- күдікті және бүлінген нысандарды карантинге орналастыру;
- SAMBA деңгейіндегі файлдық операцияларды тұтып қалу және тексеру;
- ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару;

• тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу;

- есептерді HTML және CSV форматтарында экспорттау және сақтау;
- файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын

қамтамасыз ету үшін ДК ресурстарын пайдалануды икемді басқару;

- зақымданған нысанның көшірмесін, егер ол ақпараттық құндылықты білдірсе, талап бойынша нысанды ықтимал қалпына келтіру мақсатында сауықтыру және жою алдында резервтік қоймада сақтау;
- root құқықтары жоқ қолданушының кескінді интерфейсі арқылы басқару;
- жоғарыда аталған барлық компоненттерді бірыңғай басқару жүйесі немесе веб-консоль арқылы орталықтандырылған басқару;
- қолданушылардың орнатылған немесе компьютерге қосылған құрылғыларға құрылғы түрлері мен қосылу шиналары бойынша қол жеткізуін басқару;
- алынбалы дискілерді тексеру;

- желілік шабуылдарға тән әрекеттің кіріс желілік трафигін бақылау;
- HTTP/HTTPS және FTP хаттамалары арқылы қолданушының компьютеріне келетін трафикті тексеру, сондай-ақ веб-мекенжайлардың зиянды немесе фишингке жататындығын орнату мүмкіндігі;
- пайдаланушының компьютеріндегі бағдарламалардың әрекеттері туралы мәліметтер алу;
- бағдарламаны іске қосқан кезде бақылау файлдарын жасау;
- компьютерлерде орнатылған бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу;
- автоматты іске қосу нысандарын тексеру, жүктеу секторлары, жад процессоры және ядро жады;
- сауықтыру немесе жою алдында файлдардың сақтық көшірмелерін сақтау және сақтық көшірмелерден файлдарды қалпына келтіру.

Windows ОЖ негізіндегі орталықтандырылған басқару, мониторингтеу және жаңарту бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелері басқаратын компьютерлерде жұмыс істеуі керек:

o Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядты/64-разрядты;

o Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядты/64-разрядты;

o Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядты/64-разрядты;

o Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядты/64-разрядты;

o RS5 (October 2018 Update, 1809) жұмыс станцияларына аоналған Microsoft Windows 10 Pro 32-разрядты /64-разрядты

o Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Pro 19H1 32-разрядты/64-разрядты;

o 19H1 жұмыс станцияларына арналған Microsoft Windows 10 Pro 32-разрядты/64-разрядты;

o Microsoft Windows 10 Enterprise 19H1 32-разрядты/64-разрядты;

o Microsoft Windows 10 Education 19H1 32-разрядты/64-разрядты;

o Microsoft Windows 10 Pro 19H2 32-разрядты/64-разрядты;

o 19H2 жұмыс станциясына арналған Microsoft Windows 10 Pro 32-разрядты/64-разрядты;

o Microsoft Windows 10 Enterprise 19H2 32-разрядты/64-разрядты;

o Microsoft Windows 10 Education 19H2 32-разрядты/64-разрядты;

o Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядты/64-разрядты;

o Microsoft Windows 11 Home 64-разрядты;

o Microsoft Windows 11 Pro 64-разрядты;

o Microsoft Windows 11 Enterprise 64-разрядты;

o Microsoft Windows 11 Education 64-разрядты;

o Microsoft Windows 8.1 Pro 32-разрядная/64-разрядты;

o Microsoft Windows 8.1 Enterprise 32-разрядты/64-разрядты;

o Microsoft Windows 8 Pro 32-разрядты/64-разрядты;;

o Microsoft Windows 8 Enterprise 32-разрядты/64-разрядты;

o Microsoft Windows 7 Professional Service Pack 1 32-разрядты/64-разрядты;

o Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядты/64-разрядты;

o Windows Server 2008 R2 with Standard Service Pack 1 және одан жоғары 64-разрядты;

o Windows Server 2008 R2 Service Pack 1 (барлық редакциялар) 64-разрядты;

o Windows Server 2012 Server Core 64-разрядты;

o Windows Server 2012 Datacenter 64-разрядты;

o Windows Server 2012 Essentials 64-разрядты;

o Windows Server 2012 Foundation 64-разрядты;

o Windows Server 2012 Standard 64-разрядты;

o Windows Server 2012 R2 Server Core 64-разрядты;

o Windows Server 2012 R2 Datacenter 64-разрядты;

o Windows Server 2012 R2 Essentials 64-разрядты;

o Windows Server 2012 R2 Foundation 64-разрядты;

o Windows Server 2012 R2 Standard 64-разрядты;

o Windows Server 2016 Datacenter (LTSB) 64-разрядты;

o Windows Server 2016 Standard (LTSB) 64-разрядты;

o Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядты;

o Windows Server 2019 Standard 64-разрядты;

o Windows Server 2019 Datacenter 64-разрядты;

o Windows Server 2019 Core 64-разрядты;

o Windows Server 2022 Standard 64-разрядты;

o Windows Server 2022 Datacenter 64-разрядты;

o Windows Server 2022 Core 64-разрядты;

o Windows Storage Server 2012 64-разрядты;

o Windows Storage Server 2012 R2 64-разрядты;

o Windows Storage Server 2016 64-разрядты;

o Windows Storage Server 2019 64-разрядты.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек:

o VMware vSphere 6.7;

o VMware vSphere 7.0;

o VMware Workstation 16 Pro;

o Microsoft Hyper-V Server 2012 64-разрядты;

o Microsoft Hyper-V Server 2012 R2 64-разрядты;

o Microsoft Hyper-V Server 2016 64-разрядты;

o Microsoft Hyper-V Server 2019 64-разрядты;

o Microsoft Hyper-V Server 2022 64-разрядты;

o Citrix XenServer 7.1 LTSR;

o Citrix XenServer 8.x;

o Parallels Desktop 17;

o Oracle VM VirtualBox 6.x.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі тиіс:

o Microsoft SQL Server 2012 Express 64-разрядты;

o Microsoft SQL Server 2014 Express 64-разрядты;

o Microsoft SQL Server 2016 Express 64-разрядты;

o Microsoft SQL Server 2017 Express 64-разрядты;

o Microsoft SQL Server 2019 Express 64-разрядты;

o Microsoft SQL Server 2014 (барлық редакциялары) 64-разрядты;

o Microsoft SQL Server 2016 (барлық редакциялары) 64-разрядты;

o Windows –ге арналған Microsoft SQL Server 2017 (барлық редакциялары) 64-разрядты;

o Linux-ке арналған Microsoft SQL Server 2017 (барлық редакциялары) 64-разрядты;

o Windows –ге арналған Microsoft SQL Server 2019 (барлық редакциялары 64-разрядьты (қосымша әрекеттер талап етіледі);

o Linux-ке арналған Microsoft SQL Server 2019 (барлық редакциялары 64-разрядьты (қосымша әрекеттер талап етіледі);

o Microsoft Azure SQL Database;

o Amazon RDS және Microsoft Azure бұлтты платформаларында қолдалатын барлық SQL-серверлер нұсқасы;

o MySQL 5.7 Community 32-разрядты/64-разрядты;

o MySQL Standard Edition 8.0 (релиз 8.0.20 және одан жоғары) 32-разрядты/64-разрядты;

o MySQL Enterprise Edition 8.0 (релиз 8.0.20 және одан жоғары) 32-разрядты/64-разрядты;

o MariaDB 10.5.x 32-разрядты/64-разрядты;

o MariaDB 10.4.x 32-разрядты/64-разрядты;

o MariaDB 10.3.22 және одан жоғары 32-разрядты/64-разрядты;

o MariaDB Server 10.3 InnoDB қоймасының қосалқы жүйесі бар 32-разрядты/64-разрядты;

o MariaDB Galera Cluster 10.3 InnoDB қоймасының қосалқы жүйесі бар 32-разрядты/64-разрядты;;

o MariaDB 10.1.30 және одан жоғары 32-разрядты/64-разрядты.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы к ерек:

- қорғалатын тораптар санына байланысты орталықтандырылған басқару, мониторингтеу және жаңарту қондырғысының архитектурасын таңдау;
- ұйымда компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында A
- анықталған компьютерлерді IP мекенжайы, ОЖ түрі, OU AD-да болу ережелерінің күйге келтіру;
- желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтар

- орталықтандырылған антивирустық қорғаныс бағдарламалық құралын орнату, жаңарту және жою;
- орталықтандырылған күйге келтіру, әкімшілендіру;
- қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау;
- басқару орталығы құралдарымен үйлеспейтін қосымшаларды орталықтандырылған жою (қолмен және автоматты) ;
- саясат пен міндеттерді өзгеру тарихын сақтау, алдыңғы нұсқалары қайтару мүмкіндігі;
- антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін-RPC, GPO, басқару жүйесінің құралдары, жергілікті орнату үшін-дербес орнату пакетін құру мүмкіндігі;
- пайдаланушы кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты антивирустық шешімнің параметрлерін қайта анықтайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар;
- қайта бөлу орын алатын триггерлердің иерархиялары;
- клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу;
- жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
- виртуалды машиналар желісін 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 күйге келтіру мүмкіндігімен көп деңгейлі басқару жүйесін құру;
- еркін деңгейдегі басқару серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
- басқару серверлері үшін көп жалға алуды қолдау (multi-tenancy) ;
- байланыс арналары арқылы да, машиналық ақпарат тасымалдағыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту;
- басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қатынау;
- клиенттік компьютер лицензиясын автоматты түрде тарату;
- пайдаланушылардың компьютерлерінде орнатылған БЖ мен жабдықты түгендеу;
- орнатылған антивирустық қорғаныс қосымшаларының жұмысында оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді күйге келтіру;
- Exchange ActiveSync сервері арқылы мобильді құрылғыларды басқару мүмкіндігі;
- iOS MDM сервері арқылы мобильді құрылғыларды басқару мүмкіндігі;
- берілген оқиғалар туралы SMS-хабарламаларды жіберу;
- басқарылатын ұялы құрылғыларға сертификаттарды орталықтандырылған орнату;
- басқару жүйесіне желілік жүктемені азайту үшін кез-келген ұйымның компьютерін жаңартуларды қайта жіберу орталығына бағыттау;
- ұйымның кез-келген компьютерін антивирустық агенттердің оқиғаларын бағыттау орталығы, клиенттік компьютерлердің таңдалған тобы, басқару жүйесіне желілік жүктемені азайту үшін орталықтандырылған басқару серверіне бағыттауы;
- вирусқа қарсы қорғау оқиғалары, түгендеу деректері, белгіленген бағдарламаларды лицензиялау деректері бойынша графикалық есептерді құру;
- жүйенің жұмысы туралы алдын ала күйге келтірілген стандартты есептердің болуы;
- есептерді PDF және XML форматындағы файлдарға экспорттау;
- антивирустық бағдарламалық жасақтама орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин нысанлдарын орталықтандырылған басқару;
- басқару серверінде аутентификация үшін ішкі есептік жазбаларды құру;
- басқару жүйесінің бірге құрылған басқару жүйесінің сақтық көшірмесін жасау;

• Windows Failover Clustering қолдауы;

• Windows сервисом Certificate Authority –пен бірігуін қолдлау;

- пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы;

- өзіне-өзі қызмет көрсету порталы басқару агентін ұялы құрылғыға орнату,

ұялы құрылғыларды қарау, бұғаттау командасын жіберу, құрылғыны іздеу және пайдаланушының ұялы құрылғысында деректерді жою мақсатында пайдаланушыларды қосу мүмкіндігін қамтамасыз етуі тиіс;

- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- Microsoft Azure және Google Cloud бұлтты инфрақұрылымындағы қондырғылар;
- OpenAPI интеграциясы;
- WEB консолін пайдаланып антивирустық қорғауды басқару;
- әкімшілеу консоліне рұқсатсыз кіру қаупін азайту үшін екі сатылы тексеру;
- пайдаланушы еаептік жазбасының параметрлерін өзгерткеннен кейін қосымша

аутентификацияны қолданыңыз.

- IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар

құрылғылары бар желілерді сұрау мүмкіндігі;

- әкімшілеу серверін қол жетімділігі жоғары жүйе ретінде орналастыру мүмкіндігі.

Linux ОЖ негізіндегі орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелері басқаратын компьютерлерде жұмыс істеуі керек:

o Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;

o Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная;

o Debian GNU/Linux 9.x (Stretch) 32-разрядты/64-разрядты;

o Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядты;

o Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядты;

o CentOS 7.x 64-разрядты;

o Red Hat Enterprise Linux Server 8.x 64-разрядты;

o Red Hat Enterprise Linux Server 7.x 64-разрядты;

o SUSE Linux Enterprise Server 12 (жаңартулардың барлық пакеттері) 64-разрядты;

o SUSE Linux Enterprise Server 15 (жаңартулардың барлық пакеттері) 64-разрядты;

o Astra Linux Special Edition 1.7 (тұйықталған бағдарламалық орта режімі мен мандаттық редимді қоса алғанда) 64-разрядты;

o Astra Linux Special Edition 1.6 (тұйықталған бағдарламалық орта режімі мен мандаттық редимді қоса алғанда) 64-разрядты;

o Astra Linux Common Edition 2.12 64-разрядты;

o Альт Сервер 10 64-разрядты;

o Альт Сервер 9.2 64-разрядная;

o Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядты;

o Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядты;

o Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядты;

o Oracle Linux 7 64-разрядты;

o Oracle Linux 8 64-разрядная;

o РЕД ОС 7.3 Сервер 64-разрядты;

o РЕД ОС 7.3 Сертификатталған редакция 64-разрядты.

Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек:

o VMware vSphere 6.7.

o VMware vSphere 7.0;

o VMware Workstation 16 Pro;

o Microsoft Hyper-V Server 2012 64-разрядты;

o Microsoft Hyper-V Server 2012 R2 64-разрядты;

o Microsoft Hyper-V Server 2016 64-разрядты;

o Microsoft Hyper-V Server 2019 64-разрядты;

o Microsoft Hyper-V Server 2022 64-разрядты;

o Citrix XenServer 7.1 LTSR;

o Citrix XenServer 8.x;

o Parallels Desktop 17;

o Kernel негізіндегі виртуалды машина. Келесі операциялық жүйелерді қолдайды:

o Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядты;

o Альт Сервер 10 64-разрядты;

o Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

o Debian GNU/Linux 11.x (Bullseye) 32-разрядты /64-разрядты;

o Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядты;

o РЕД ОС 7.3 Сервер 64-разрядты;

o РЕД ОС 7.3 Сертификатталған редакция 64-разрядты

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі керек:

o MySQL 5.7 Community 32-разрядты/64-разрядты;

o MySQL 8.0 32-разрядная/64-разрядная;

o MariaDB 10.5.x 32-разрядты/64-разрядты;

o MariaDB 10.4.x 32-разрядты/64-разрядты;

o MariaDB 10.3.22 және одан жоғары 32-разрядты/64-разрядты;

o MariaDB Server 10.3 32-разрядты/64-разрядты InnoDB қоймасының қосалқы жүйесімен;

o MariaDB 10.1.30 және одан жоғары 32-разрядты/64-разрядты.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы к ерек:

- антивирустық қорғаныс бағдарламалық құралын орталықтандырылған орнату, жаңарту және жою;
- орталықтандырылған күйге келтіру, әкімшілендіру;
- қорғаныс құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау;
- саясат пен міндеттерді өзгеру тарихын сақтау, алдыңғы нұсқалары қайтару мүмкіндігі;
- антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін-RPC, GPO, басқару жүйесінің құралдары, жергілікті орнату үшін-дербес орнату пакетін құру мүмкіндігі;
- қайта бөлу орын алатын триггерлердің иерархиялары;
- жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
- виртуалды машиналар желісін 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 күйге келтіру мүмкіндігімен көп деңгейлі басқару жүйесін құру;
- еркін деңгейдегі басқару серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
- басқару серверлері үшін көп жалға алуды қолдау (multi-tenancy) ;
- байланыс арналары арқылы да, машиналық ақпарат тасымалдағыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту;
- басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қатынау;
- клиенттік компьютер лицензиясын автоматты түрде тарату;
- орнатылған антивирустық қорғаныс қосымшаларының жұмысында оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді күйге келтіру;
- вирусқа қарсы қорғау оқиғалары, түгендеу деректері, белгіленген бағдарламаларды лицензиялау деректері бойынша графикалық есептерді құру;
- жүйенің жұмысы туралы алдын ала күйге келтірілген стандартты есептердің болуы;
- есептерді PDF және XML форматындағы файлдарға экспорттау;
- антивирустық бағдарламалық жасақтама орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин нысанлдарын орталықтандырылған басқару;
- басқару серверінде аутентификация үшін ішкі есептік жазбаларды құру;
- басқару жүйесінің бірге құрылған басқару жүйесінің сақтық көшірмесін жасау;
- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- WEB консолін пайдаланып антивирустық қорғауды басқару;
- басқару серверіне жүктемені азайту және кәсіпорын желісіндегі деректер трафигін

оңтайландыру үшін басқару сервері арқылы да, тарату нүктелері арқылы да басқарылатын құрылғыларда антивирустық базалар мен бағдарламалық модульдерді жаңарту және тарату мүмкіндігі;

- жаңартуларды тексеру тапсырмасы арқылы жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын өнімділік пен қателерінің болуын тексеру мүмкіндігі;
- антивирустық базалар мен бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары мүмкіндігін пайдалану мүмкіндігі.

Антивирустық базаларды жаңартуға қойылатын талаптар

Жаңартылатын антивирустық мәліметтер базасы келесі функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс

- күнтізбелік тәулік ішінде кемінде 24 рет антивирустық базаларды жаңарту қағидаларын құру;
- жаңарту жолдарының көптігі, оның ішінде-байланыс арналары бойынша және иеліктен шығарылатын электрондық ақпарат тасымалдағыштарда;
- электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру.

Пайдалану құжаттамасына қойылатын талаптар

Басқару құралдарын қоса алғанда, антивирустық қорғаныстың барлық бағдарламалық өнімдері үшін пайдалану құжаттамасында Мемлекеттік стандарттардың талаптарына сәйкес орыс тілінде дайындалған құжаттар қамтылуға тиіс, оның ішінде:

- "Пайдаланушы (әкімші) нұсқаулығы"

Антивирустық құралдармен бірге жеткізілетін құжаттама тиісті антивирустық қорғаныс құралын орнату, күйге келтіру және пайдалану үрдісін егжей-тегжейлі сипаттауы керек.

Техникалық қолдауға қойылатын талаптар

Антивирустық бағдарламалық жасақтаманы техникалық қолдау:

- Қазақстан Республикасының бүкіл аумағында антивирустық қорғау құралдарын өндірушінің және оның серіктестерінің сертификатталған мамандары электрондық пошта және Интернет арқылы орыс тілінде ұсынуға міндетті.
- Антивирустық шешім өндірушісінің Web -сайты орыс тілінде болуы керек, антивирустық шешімді техникалық қолдауға арналған арнайы бөлім, толықтырылатын білім базасы, сондай-ақ бағдарламалық өнімдерді пайдаланушылар форумы болуы керек

2. ҰСЫНЫЛАТЫН ҚЫЗМЕТ КӨЛЕМІ.

1-кесте:

№	Атауы	Лицензиялар саны

1	Кешенді антивирустық шешім, пайдалануға жазылу мерзімі лицензиялар орналастырылған күннен бастап 12 айдан кем емес мерзімді құрауы тиіс	10

3. ҚЫЗМЕТ КӨРСЕТУ ШАРТТАРЫ ЖӘНЕ ОҒАН ҚОЙЫЛАТЫН ТАЛАПТАР

Әлеуетті жеткізуші Қазақстан Республикасының аумағында өндірушіден не өндірушінің ресми дистрибьюторынан және Қазақстан Республикасының аумағында сатып алынатын құқық иеленушінің лицензияларын пайдалануға айрықша емес құқықтарды сатуға құқығын растайтын бағдарламалық жасақтаманы жеткізуге авторизациялық хат ұсынуға тиіс.

3. Сатып алынатын ТЖҚ жеке әлеуетті жеткізушіге немесе өндірушіге тиістілігін анықтайтын сипаттамалар бар

тауарларды, жұмыстарды және көрсетілетін қызметтерді қосымша жинақтау, қосымша жарақтандыру, біріздендіру немесе қолда бар тауарлармен, жұмыстармен және көрсетілетін қызметтермен үйлесімділігін қамтамасыз ету үшін, сондай-ақ одан әрі техникалық сүйемелдеу, сервистік қызмет көрсету және жөндеу, оның ішінде негізгі (орнатылған) жабдықты жоспарлы жөндеу (қажет болған кезде) үшін сатып алу

Қол қойған Мурзагулова Махабат Кабиденовна
Қол қойылған күні 12.09.2024

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1027681
способом Запрос ценовых предложений на понижение

Лот № 1 (116-1 У, 3753579) Услуги по продлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "QazCloud (КазКлауд)"

Организатор: Товарищество с ограниченной ответственностью "QazCloud (КазКлауд)"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	116-1 У
Наименование и краткая характеристика	Услуги по продлению лицензий на право использования программного обеспечения, Услуги по продлению лицензий на право использования программного обеспечения
Дополнительная характеристика	-
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Астана, пр.Мангилик ел 35А
Условия поставки	-
Срок поставки	С даты подписания договора в течение 15 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

РАЗДЕЛ I. ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Услуга по продлению права пользования лицензионного программного обеспечения (антивирус)

Услуга по продлению права пользования лицензионного программного обеспечения (далее - ПО) должна быть предоставлена в электронном виде на электронный адрес Заказчика.

1. ОПИСАНИЕ И ТРЕБУЕМЫЕ ТЕХНИЧЕСКИЕ, КАЧЕСТВЕННЫЕ И ЭКСПЛУАТАЦИОННЫЕ ХАРАКТЕРИСТИКИ ПРЕДОСТАВЛЯЕМОЙ УСЛУГИ.

Услуга по продлению права использования лицензионного программного обеспечения (антивирус) предусматривает использование лицензионного ПО, согласно Таблице №1 (передачу неисключительных прав на использование программного обеспечения), с условием единовременной оплаты.

Наименования лицензионного программного обеспечения (антивирус): Kaspersky Endpoint Security for Business - Select Kazakhstan Edition. 10-14 Node 1 year Base License.

Общие требования

Антивирусные средства должны включать:

программные средства антивирусной защиты для рабочих станций и серверов Windows;

программные средства антивирусной защиты для рабочих станций и серверов Linux;

программные средства централизованного управления, мониторинга и обновления;

обновляемые базы данных сигнатур вредоносных программ и атак;

эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

Требования к программным средствам антивирусной защиты для рабочих станций Windows

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:

o Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;

o Windows 8 Professional / Enterprise (32 / 64-разрядная);

o Windows 8.1 Professional / Enterprise (32 / 64-разрядная);

o Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;

o Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise.

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

• антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;

• антивирусное сканирование по расписанию;

• антивирусное сканирование подключаемых устройств;

• эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;

• нейтрализации действий активного заражения;

• анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;

• анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

• блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;

• откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;

• ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;

• облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

• антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

• защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;

• фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;

• проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;

• блокировку баннеров и всплывающих окон на загружаемых Web-страницах;

• распознавания и блокировку фишинговых и небезопасных сайтов;

• встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;

• защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;

• защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;

• контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;

• создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;

• 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 Active Directory;

• управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;

• записи в журнал событий о записи и/или удалении файлов на съемных дисках;

• назначение приоритета для правил доступа к устройствам с файловой системой;

• контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;

• защиты от атак типа BadUSB;

• запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

• защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;

• управления параметрами через доверенные программы удаленного администрирования;

• установки только выбранных компонентов программного средства антивирусной защиты;

• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

• запуска задач по расписанию и/или сразу после запуска приложения;

• гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

• ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• проверки целостности антивирусной программы;

• добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;

• импорта и экспорта списков правил и исключений в XML-формат;

• наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

• наличие защищенного хранилища для отчетов о работе антивируса;

• включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;

• интеграции с Windows Defender Security Center;

• наличие поддержки Antimalware Scan Interface (AMSI);

• наличие поддержки Windows Subsystem for Linux (WSL);

• защитить паролем восстановление объектов из резервного хранилища;

• ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;

• наличие инструмента мониторинга сети по протоколам TCP и UDP;

• возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;

• возможность установки ограничение длительности выполнения задачи;

• возможность ставить задачи проверки в очередь, если проверка уже выполняется.

Требования к программным средствам антивирусной защиты для серверов Windows

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий:

o Windows Small Business Server 2011 Essentials / Standard (64-разрядная), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2;

o Windows MultiPoint Server 2011 (64-разрядная);

o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;

o Windows Server 2012 Foundation / Essentials / Standard / Datacenter;

o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;

o Windows Server 2016 Essentials / Standard / Datacenter;

o Windows Server 2019 Essentials / Standard / Datacenter;

o Windows Server 2022.

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

• антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;

• антивирусное сканирование по расписанию;

• антивирусное сканирование подключаемых устройств;

• эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;

• нейтрализации действий активного заражения;

• анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;

• анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

• блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;

• откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;

• облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

• антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

• встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;

• защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;

• запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

• защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;

• установки только выбранных компонентов программного средства антивирусной защиты;

• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

• ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• проверки целостности антивирусной программы;

• добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;

• наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

• наличие защищенного хранилища для отчетов о работе антивируса;

• включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;

• интеграции с Windows Defender Security Center;

• наличие поддержки Antimalware Scan Interface (AMSI);

• наличие поддержки Windows Subsystem for Linux (WSL);

• защитить паролем восстановление объектов из резервного хранилища.

• импорта и экспорта списков правил и исключений в XML-формат;

• ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;

• возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;

• возможность установки ограничения длительности выполнения задачи;

• возможность ставить задачи проверки в очередь, если проверка уже выполняется.

Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 32-битных операционных систем следующих версий:

o CentOS 6.7 и выше.

o Debian GNU/Linux 10.1 и выше.

o Debian GNU/Linux 11.

o Mageia 4.

o Red Hat Enterprise Linux 6.7 и выше.

o Альт 8 СП Рабочая Станция.

o Альт 8 СП Сервер.

o Альт Образование 10.

o Альт Рабочая Станция 10.

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:

o AlmaLinux OS 8 и выше.

o AlmaLinux OS 9 и выше.

o AlterOS 7.5 и выше.

o Amazon Linux 2.

o Astra Linux Common Edition 2.12.

o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).

o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).

o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).

o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).

o CentOS 6.7 и выше.

o CentOS 7.2 и выше.

o CentOS Stream 9.

o Debian GNU/Linux 10.1 и выше.

o Debian GNU/Linux 11.

o EMIAS 1.0.

o EulerOS 2.0 SP5.

o LinuxMint 19.2 и выше.

o LinuxMint 20.3 и выше.

o openSUSE Leap 15.0 и выше.

o Oracle Linux 7.3 и выше.

o Oracle Linux 8.0 и выше.

o Red Hat Enterprise Linux 6.7 и выше.

o Red Hat Enterprise Linux 7.2 и выше.

o Red Hat Enterprise Linux 8.0 и выше.

o Red Hat Enterprise Linux 9.

o Rocky Linux 8.5 и выше.

o SUSE Linux Enterprise Server 12.5 и выше.

o SUSE Linux Enterprise Server 15 и выше.

o Ubuntu 20.04 LTS.

o Ubuntu 22.04 LTS.

o Альт 8 СП Рабочая станция.

o Альт 8 СП Сервер.

o Альт Образование 10.

o Альт Рабочая Станция 10.

o Альт Сервер 10.

o Атлант, сборка Alcyone, версия 2022.02.

o Гослинукс 7.17.

o Гослинукс 7.2.

o РЕД ОС 7.3.

o РОСА "Кобальт" 7.9.

o РОСА "Хром" 12.

o ОСОН "ОСНова".

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

o Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).

o EulerOS 2.0 SP8.

o SUSE Linux Enterprise Server 15 SP3.

o Ubuntu 20.04 LTS.

о Альт 8 СП Сервер.

о РЕД ОС 7.3.

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

• резидентного антивирусного мониторинга;

• облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

• проверку ресурсов доступных по SMB / NFS;

• возможность проверки памяти ядра;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;

• проверку 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);

• защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;

• включения опции блокирования файлов во время проверки;

• помещение подозрительных и поврежденных объектов на карантин;

• перехвата и проверки файловых операций на уровне SAMBA;

• управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• экспортировать и сохранять отчеты в форматах HTML и CSV;

• гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

• сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;

• управления через пользовательский графический интерфейс без root прав;

• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;

• управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;

• проверки съемных дисков;

• отслеживания во входящем сетевом трафике активности, характерной для сетевых атак

• проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым;

• получения данных о действиях программ на компьютере пользователя;

• создание файлов трассировки при запуске программы;

• получение информации обо всех исполняемых файлах программ, установленных на компьютерах;

• проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;

• сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий.

Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

o Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;

o Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 11 Home 64-разрядная;

o Microsoft Windows 11 Pro 64-разрядная;

o Microsoft Windows 11 Enterprise 64-разрядная;

o Microsoft Windows 11 Education 64-разрядная;

o Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;

o Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;

o Microsoft Windows 8 Pro 32-разрядная/64-разрядная;

o Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;

o Microsoft Windows 7 Professional Service Pack 1 32-разрядная/64-разрядная;

o Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная;

o Windows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;

o Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;

o Windows Server 2012 Server Core 64-разрядная;

o Windows Server 2012 Datacenter 64-разрядная;

o Windows Server 2012 Essentials 64-разрядная;

o Windows Server 2012 Foundation 64-разрядная;

o Windows Server 2012 Standard 64-разрядная;

o Windows Server 2012 R2 Server Core 64-разрядная;

o Windows Server 2012 R2 Datacenter 64-разрядная;

o Windows Server 2012 R2 Essentials 64-разрядная;

o Windows Server 2012 R2 Foundation 64-разрядная;

o Windows Server 2012 R2 Standard 64-разрядная;

o Windows Server 2016 Datacenter (LTSB) 64-разрядная;

o Windows Server 2016 Standard (LTSB) 64-разрядная;

o Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;

o Windows Server 2019 Standard 64-разрядная;

o Windows Server 2019 Datacenter 64-разрядная;

o Windows Server 2019 Core 64-разрядная;

o Windows Server 2022 Standard 64-разрядная;

o Windows Server 2022 Datacenter 64-разрядная;

o Windows Server 2022 Core 64-разрядная;

o Windows Storage Server 2012 64-разрядная;

o Windows Storage Server 2012 R2 64-разрядная;

o Windows Storage Server 2016 64-разрядная;

o Windows Storage Server 2019 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

o VMware vSphere 6.7;

o VMware vSphere 7.0;

o VMware Workstation 16 Pro;

o Microsoft Hyper-V Server 2012 64-разрядная;

o Microsoft Hyper-V Server 2012 R2 64-разрядная;

o Microsoft Hyper-V Server 2016 64-разрядная;

o Microsoft Hyper-V Server 2019 64-разрядная;

o Microsoft Hyper-V Server 2022 64-разрядная;

o Citrix XenServer 7.1 LTSR;

o Citrix XenServer 8.x;

o Parallels Desktop 17;

o Oracle VM VirtualBox 6.x.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

o Microsoft SQL Server 2012 Express 64-разрядная;

o Microsoft SQL Server 2014 Express 64-разрядная;

o Microsoft SQL Server 2016 Express 64-разрядная;

o Microsoft SQL Server 2017 Express 64-разрядная;

o Microsoft SQL Server 2019 Express 64-разрядная;

o Microsoft SQL Server 2014 (все редакции) 64-разрядная;

o Microsoft SQL Server 2016 (все редакции) 64-разрядная;

o Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;

o Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;

o Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная (требуются дополнительные действия);

o Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия);

o Microsoft Azure SQL Database;

o Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;

o MySQL 5.7 Community 32-разрядная/64-разрядная;

o MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;

o MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;

o MariaDB 10.5.x 32-разрядная/64-разрядная;

o MariaDB 10.4.x 32-разрядная/64-разрядная;

o MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;

o MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

o MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

o MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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

• выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;

• чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;

• 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;

• 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;

• 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;

• поддержка мультиарендности (multi-tenancy) для серверов управления;

• 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;

• отправки SMS-оповещений о заданных событиях;

• централизованная установка сертификатов на управляемые мобильные устройства;

• указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;

• указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;

• 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;

• 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;

• портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;

• наличие системы контроля возникновения вирусных эпидемий;

• установки в облачной инфраструктуре Microsoft Azure и Google Cloud;

• интеграции по OpenAPI;

• управления антивирусной защитой с использованием WEB консоли;

• двухэтапная проверка 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.

Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

o Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;

o Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная;

o Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная;

o Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;

o Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная;

o CentOS 7.x 64-разрядная;

o Red Hat Enterprise Linux Server 8.x 64-разрядная;

o Red Hat Enterprise Linux Server 7.x 64-разрядная;

o SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная;

o SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная;

o Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

o Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

o Astra Linux Common Edition 2.12 64-разрядная;

o Альт Сервер 10 64-разрядная;

o Альт Сервер 9.2 64-разрядная;

o Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;

o Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная;

o Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная;

o Oracle Linux 7 64-разрядная;

o Oracle Linux 8 64-разрядная;

o РЕД ОС 7.3 Сервер 64-разрядная;

o РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

o VMware vSphere 6.7.

o VMware vSphere 7.0;

o VMware Workstation 16 Pro;

o Microsoft Hyper-V Server 2012 64-разрядная;

o Microsoft Hyper-V Server 2012 R2 64-разрядная;

o Microsoft Hyper-V Server 2016 64-разрядная;

o Microsoft Hyper-V Server 2019 64-разрядная;

o Microsoft Hyper-V Server 2022 64-разрядная;

o Citrix XenServer 7.1 LTSR;

o Citrix XenServer 8.x;

o Parallels Desktop 17;

o Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:

o Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;

o Альт Сервер 10 64-разрядная;

o Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

o Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;

o Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;

o РЕД ОС 7.3 Сервер 64-разрядная;

o РЕД ОС 7.3 Сертифицированная редакция 64-разрядная

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

o MySQL 5.7 Community 32-разрядная/64-разрядная;

o MySQL 8.0 32-разрядная/64-разрядная;

o MariaDB 10.5.x 32-разрядная/64-разрядная;

o MariaDB 10.4.x 32-разрядная/64-разрядная;

o MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;

o MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

o MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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

• централизованные установка, обновление и удаление программных средств антивирусной защиты;

• централизованная настройка, администрирование;

• просмотр отчетов и статистической информации по работе средств защиты;

• сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;

• иерархии триггеров, по которым происходит перераспределение;

• 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;

• поддержка мультиарендности (multi-tenancy) для серверов управления;

• 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;

• наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;

• построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;

• наличие преднастроенных стандартных отчетов о работе системы;

• экспорт отчетов в файлы форматов PDF и XML;

• 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;

• наличие системы контроля возникновения вирусных эпидемий;

• управления антивирусной защитой с использованием WEB консоли;

• возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;

• возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;

• возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули.

Требования к обновлению антивирусных баз

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 каналам связи и на отчуждаемых электронных носителях информации;

• проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

• «Руководство пользователя (администратора)»

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

• Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Республики Казахстан по электронной почте и через Интернет.

• Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

2. ОБЪЕМ ПРЕДОСТАВЛЯЕМОЙ УСЛУГИ.

Таблица 1:

№	Наименование	Количество лицензий
1	Комплексное антивирусное решение, срок подписки на использования должен составлять не менее 12 месяцев, с даты размещения лицензий	10

3. УСЛОВИЯ И ТРЕБОВАНИЯ К ОКАЗАНИЮ УСЛУГИ

Потенциальный поставщик должен предоставить авторизационное письмо от производителя либо официального дистрибьютора производителя на территории РК и на поставку программного обеспечения, подтверждающего право на продажу неисключительных прав на использование лицензий закупаемого ПО правообладателя на территории Республики Казахстан.

3. Присутствует указание характеристик, определяющих принадлежность приобретаемого ТРУ отдельному потенциальному поставщику либо производителю на основании

приобретения товаров, работ и услуг для доукомплектования, дооснащения, унификации или обеспечения совместимости с имеющимися товарами, работами и услугами, а также для дальнейшего технического сопровождения, сервисного обслуживания и ремонта, в том числе планового ремонта (при необходимости), основного (установленного) оборудования

Подписал	Мурзагулова Махабат Кабиденовна
Дата подписания	12.09.2024