ТЕХНИКАЛЫҚ СИПАТТАМА

1271455 сатып алу бойынша
Бағалы ұсыныстарға сұраным тәсілімен

Лот № (418 У, 4583627) Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер

Тапсырыс беруші: "Ауыл Телеком" жауапкершілігі шектеулі серіктестігі

Ұйымдастырушы: "Қазақтелеком" акционерлік қоғамының филиалы "Телеком Жинақтау" дирекциясы"

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	418 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, Алматы қ.
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 10 жұмыс күніішінде
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

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

Өңделетін ақпараттың құпиялылық дәрежесіне қарамастан, бүкіл ұйым бойынша бірыңғай антивирустық құралдар қолданылуы тиіс. Дербес тұрған, яғни вирусқа қарсы қорғаныстың бірыңғай жүйесіне қосылмаған, оның ішінде шалғай аумақтардағы дербес компьютерлер зиянды бағдарламалардың және желілік шабуылдардың барлық түрлерінен қорғауды қамтитын интеграцияланған бағдарламалық өніммен қорғалуы және олардың бірыңғай жүйеге қосылу мүмкіндігін қамтамасыз етуі тиіс. вирусқа қарсы қорғаныс.

Атауы ұзартылатын лицензиялар: Kaspersky Endpoint Security for Business Advanced

Ағымдағы лицензиялық келісімнің нөмірі: 1FF0-251120-104157-833-1648

Жұмыс станциялары мен файлдық жүйелерді қорғауға арналған лицензиялардың саны: 100

Лицензияның қолданылу мерзімі: 12 күнтізбелік ай

Техникалық қолдаудың жарамдылық мерзімі: кемінде 1 (бір) жыл

Лицензия түрі: корпоративтік (100 жұмыс станциясына 1 кілт).

Әлеуетті өнім берушіге қойылатын талаптар:

Контрафактілік бағдарламалық қамтамасыз етуді жеткізуді болдырмау мақсатында әлеуетті жеткізуші өндіруші компаниядан бағдарламалық қамтамасыз етудің заңды түрде шыққанын растайтын хатты ұсынуы тиіс.

Қораптағы редакция қабылданбайды.

Жалпы талаптар

Вирусқа қарсы құралдар мыналарды қамтуы тиіс:

» Windows жұмыс станцияларына арналған антивирустық бағдарламалық қамтамасыздандыру құралдары;

» Windows файлдық серверлеріне арналған антивирустық бағдарламалық қамтамасыздандыру;

» Mac жұмыс станцияларына арналған антивирустық бағдарламалық қамтамасыздандыру;

» Linux жұмыс станциялары мен серверлеріне арналған антивирустық бағдарламалық қамтамасыздандыру;

» мобильді құрылғыларға (смартфондар мен планшеттерге) арналған антивирустық қорғаудың бағдарламалық құралдары;

» орталықтандырылған басқарудың, мониторингілеудің және жаңартудың бағдарламалық құралдары;

» зиянды бағдарламалар қолтаңбаларының және шабуылдардың жаңартылатын дерекқорлары;

» пайдалану құжаттамасы орыс тілінде.

Барлық антивирустық құралдардың, оның ішінде басқару элементтерінің бағдарламалық интерфейсі орыс және ағылшын тілдерінде болуы керек.

Барлық антивирустық құралдар, соның ішінде басқару элементтері, орыс және ағылшын тілдерінде контексттік анықтамалық жүйеге ие болуы керек.

Windows жұмыс станцияларына арналған антивирустық бағдарламалық қамтамасыздандыруға қойылатын талаптар

Вирусқа қарсы қорғаныстың бағдарламалық құралдары операциялық жүйенің басқаруымен жұмыс істейтін компьютерлерде келесі нұсқалардың жұмыс станциялары үшін жұмыс істеуі тиіс:

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

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

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

o Windows 10 Home / Pro / Pro үшін жұмысшылардың станциялардың / Education / Enterprise/Enterprise multi-session;

o Windows 11 Home / Pro / Pro үшін жұмысшылардың станциялардың / Education / Enterprise;

o Windows 11 үшін Arm64 Home / Pro / Pro үшін жұмысшылардың станциялардың / Education / Enterprise.

Антивирустық қорғаудың бағдарламалық жасақтамасында келесі функционалдық мүмкіндіктер орындалуы керек:

· нақты уақыт режимінде және объектінің контекстік мәзірінен сұраныс бойынша антивирустық сканерлеу;

· кесте бойынша антивирустық сканерлеу;

· қосылатын құрылғыларды вирусқа қарсы сканерлеу;

· бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;

· белсенді залалдану әрекеттерін бейтараптандыру;

· қолданбаның әрекетін және оның зиянды әрекетін анықтау және рұқсат етілмеген әрекеттерді анықтау үшін жүйедегі әрекеттерін талдау;

· желі арқылы қолжетімді қорғалған ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қол жеткізуді талдау;

· жалпыға қолжетімді қалталарды сыртқы шифрлаудан қорғау функциясы үшін қорғау аймағын конфигурациялаңыз;

· бағдарламалық қамтамасыз етудегі осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, соның ішінде жүйелік процестердің жадын қорғау;

· шифрланған, зиянды бағдарламаларды, файлдарды қалпына келтіруді қоса алғанда, емдеу кезінде зиянды бағдарламалық қамтамасыз етудің әрекеттерін кері қайтару;

· процестер мен қолданбаларға арналған артықшылықтар шектеулері (тізілімге енгізу, файлдарға, қалталарға және басқа процестерге қол жеткізу, тапсырмаларды жоспарлаушыға

қол жеткізу, құрылғыларға қол жеткізу, нысан құқықтарын өзгерту, т.б.), динамикалық түрде жаңартылатын теңшелетін тізімдер сенімділік деңгейін анықтайтын қолданбалар;

· жаңа қауіптерден бұлттық қорғаныс, бұл қолданбаға іске қосылған бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің ресурстарына қол жеткізуге мүмкіндік береді;

· келесі форматтағы архивтердегі файлдарды антивирустық тексеру және емдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

· IMAP, SMTP, POP3, MAPI, NNTP хаттамалары бойынша жіберілетін кіріс және шығыс трафикті тексере отырып, 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 протоколдары арқылы пайдаланушының компьютеріне келетін желілік трафикті, оның ішінде сенімді ресурстарды конфигурациялау мүмкіндігімен эвристикалық талдауды қолдану арқылы тексеру. блоктау немесе статистикалық режимде жұмыс істеу;

· жүктелетін веб-беттердегі баннерлер мен қалқымалы терезелерді блоктау;

· фишингтік және қауіпті сайттарды тану және бұғаттау;

· желілік сегменттерді санаттарға бөлу мүмкіндігімен желілік пакеттік ережелерді және бағдарламаларға арналған желілік ережелерді жасауға мүмкіндік беретін кіріктірілген желілік қалқан;

· кез келген түрдегі есептеу желілеріндегі қолданбалар мен порттарға арналған желілік қалқан ережелерін пайдалана отырып, желілік шабуылдардан қорғау;

· құрылғының MAC мекенжайын бұрмалау үшін ARP протоколындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;

· бір уақытта бірнеше желілік қосылымдарды орнатуды блоктау мүмкіндігімен желілік көпір сияқты желілік қосылымдарды басқару;

· барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді жасау үшін құрамдас бағдарламаны табу жолында, метадеректерде, сертификатта немесе оның саусақ ізінде, бақылау сомасында, сондай-ақ бағдарламалық құрал өндірушісі қамтамасыз ететін қолданбалардың алдын ала анықталған санаттары бойынша құрамдас қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе блоктау режимінде жұмыс істеуі керек;

· пайдаланушының сыртқы енгізу/шығару құрылғыларымен жұмысын құрылғы түрі және /немесе пайдаланылатын шина бойынша, олардың идентификаторы бойынша сенімді құрылғылардың тізімін жасау мүмкіндігімен және белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану артықшылықтарын беру мүмкіндігімен басқару. белсенді каталог;

· МТҚ құрылғыларын басқару және құрылғыларды басқару бөлігі ретінде барлық немесе пайдаланушы топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін осы түрдегі құрылғыларға қол жеткізу ережелерін конфигурациялау;

· алынбалы дискілердегі файлдарды жазу және/немесе жою туралы оқиғалар журналының жазбалары;

· файлдық жүйесі бар құрылғыларға қатынасу ережелеріне басымдық беру;

· пайдаланушының Интернетпен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық түрде жаңартып отыратын санатқа, сондай-ақ ақпарат түріне (аудио, видео және т.б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, уақыт аралықтарын енгізуге мүмкіндік беру. бақылау, сондай-ақ оны тек Active Directory-ден белгілі бір пайдаланушыларға тағайындау;

· типті шабуылдардан қорғау BadUSB;

· қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ құпия сөзді пайдаланып қолданба параметрлеріне кіруді қорғау;

· параметрлерді сенімді қашықтан басқару бағдарламалары арқылы басқару;

· вирусқа қарсы қорғау бағдарламалық құралының таңдалған құрамдастарын ғана орнату;

· жоғарыда аталған барлық құрамдастарды бірыңғай басқару жүйесі арқылы орталықтандырылған басқару;

· тапсырмаларды кесте бойынша және/немесе қолданбаны іске қосқаннан кейін бірден іске қосу;

· файлдық кеңістікті сканерлеуді орындау кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютерлік ресурстарды пайдалануды икемді басқару;

· өткен тексеруден бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жылдамдату;

· антивирустық бағдарламаның тұтастығын тексеру;

· файлдың бақылау сомасы, аты/каталог маскасы бойынша немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктерді қосу;

· ережелер мен ерекшеліктер тізімдерін XML пішіміне импорттау және экспорттау;

· антивирустың жойылған вирус жұққан файлдарды қалпына келтіру мүмкіндігімен қорғалған қоймасының болуы;

· антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы;

· антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ ең аз мүмкіндіктер жиынтығымен графикалық интерфейстің жеңілдетілген нұсқасының болуы;

· интеграциялар бастап Windows Defender Security Center;

· болуы қолдауды Antimalware Scan Interface (AMSI);

· болуы қолдауды Windows Subsystem for Linux (WSL);

· сақтық көшірме қоймасынан нысандарды қалпына келтіруді құпия сөзбен қорғаңыз;

· интернетке қосылу лимитті болып табылған жағдайда желілік трафиктің шектеулері;

· хаттамалар бойынша желіні мониторингілеу құралының болуы TCP және UDP;

· тексеру тоқтатылған жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;

· тапсырманың орындалу ұзақтығын шектеу параметрлері;

· тексеру әлдеқашан орындалып жатқан болса, тексеру тапсырмаларын кезекке қою мүмкіндігі;

· жүйені қайта іске қоспай жаңарту;

· пайдаланушылардың қолданбадағы мобильді құрылғыларға қол жеткізуін теңшеу Android Debug Bridge (ADB);

· мобильді құрылғыға кіруге тыйым салынған болса да, құрылғыны компьютерге USB арқылы қосу арқылы мобильді құрылғыны зарядтаңыз;

· пайдаланушылар үшін басып шығару құқықтарын теңшеңіз;

· желілерге қосылуды бақылау үшін WPA3 протоколының қолдауының болуы Wi-Fi;

· Azure WVD жүйесімен үйлесімділіктің болуы;

· пайдаланушылардың қолданбадағы мобильді құрылғыларға қол жеткізуін теңшеу iTunes;

· анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қолданбалардағы осалдықтарды анықтау және жабу үшін арнайы тапсырманы іске қосу.

· толық дискілі арнайы жүктеу агентін құру және Single технологиясын қолдау арқылы шифрлау Sign On, UEFI-жүйелерді қолдау;

· жүктеу агенті немесе ОЖ файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI жүйелерін қолдау;

· екі факторлы аутентификацияны қолдау кезінде толық дискілі шифрлауда;

· шифрланатын мазмұнды икемді түрде көрсету мүмкіндігімен файлдарды шифрлау (орналасқан жері, кеңейтімі, файл жасаушы қолданбасы бойынша);

· таңдалған қолданбалар тарапынан шифрланған файлдарға қолжетімділікті шектеу тетіктерінің болуы, сондай-ақ құпия сөз арқылы ұйымнан тыс файлдардың шифрын шешуге мүмкіндік беретін технологияның болуы;

· ұйым желісінен тыс файлдарды шифрлауға және шифрын ашуға мүмкіндік беретін жұмыс режимін орнату мүмкіндігімен алынбалы құралдардағы деректерді шифрлау;

· мінез-құлық үлгісінен ауытқыған жағдайда бағдарламалардың мінез-құлық үлгісін қалыптастыру және олардың әрекеттерін блоктау мүмкіндігі (ауытқуларды адаптивті бақылау)

· дискіні шифрлау кезінде аутентификация агентінің қызметтік тіркелгісін жасау мүмкіндігі;

· үшінші тараптың тіркелгі деректерін жеткізушіге қолдау көрсету ADSelfService Plus кезінде SSO жұмысы үшін толық дискілі шифрлауда;

· ерекшеліктерді орнату және енгізу құрылғыларынан басқа барлық Bluetooth құрылғыларына кіруді шектеу мүмкіндігі;

· операциялық жүйені қайта іске қоспай-ақ қолданбаны жаңарту мүмкіндігі;

· зиянды бағдарламаны іздеу тапсырмасы үшін процессор ресурстарын тұтынуды шектеу мүмкіндігі;

· қолданба қызметтерін сырттан басқаруға тыйым салу мүмкіндігі;

· тексеруден алдын ала орнатылған ерекшеліктерді және сенімді қолданбаларды таңдау мүмкіндігі;

· жеке пайдаланушыға параметрлерді конфигурациялық файлға экспорттауға рұқсатты орнату мүмкіндігі;

· құпия сөздердің тарихын (30 күнге дейін) сақтауға және күйді (Белсенді) басқаруға мүмкіндік беретін қолданбаға кіру үшін уақытша құпия сөздерді бақылау және қайтарып алу мүмкіндігі, Мерзімі өткен, қайтарып алынды);

· саясат қолданылғаннан кейін бірден веб-бақылау ережелерімен тыйым салынған веб-ресурстармен байланысты үзу мүмкіндігі;

· орнату бумасында операциялық жүйелердің әртүрлі типтері үшін құрамдастардың әртүрлі жинақтарын конфигурациялау мүмкіндігі;

· тексеруден алдын ала орнатылған ерекшеліктерді және сенімді қолданбаларды таңдау мүмкіндігі;

· ескірген TLS 1.0 протоколы бойынша желілік қосылыстарды бұғаттау мүмкіндігі;

· хаттаманы қолдау Kerberos интернетке қол жеткізу үшін прокси-сервер арқылы қосымшаның аутентификациясы үшін;

· көрсету мүмкіндігі хэш қосымшаны тексеруден шығаруға арналған файл.

Windows серверлеріне арналған антивирустық бағдарламалық қамтамасыздандыруға қойылатын талаптар

Вирусқа қарсы қорғаныстың бағдарламалық құралдары мынадай нұсқалардағы файлдық серверлерге арналған операциялық жүйенің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

o Windows Small Business Server 2011 Essentials / Standard (64-разрядная), Microsoft Small Business Server 2011 Standard (64-разрядная) қолдау көрсетіледі тек қана бастап белгіленген Service Pack 1 үшін Microsoft Windows Server 2008 R2;

o Windows MultiPoint Server 2011 (64 биттік);

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

o Windows Web Server 2008 R2 Service Pack 1 и жоғары;

o Windows Server 2012 Foundation / Essentials / Standard / Datacenter (қоса алғанда режим Server Core);

o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (қоса алғанда режим Server Core);

o Windows Server 2016 Essentials / Standard / Datacenter (қоса алғанда режим Server Core);

o Windows Server 2019 Essentials / Standard / Datacenter (қоса алғанда режим Server Core);

o Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (қоса алғанда режим Server Core).

o Windows Server 2025 Standard / Datacenter.

Антивирустық қорғаудың бағдарламалық жасақтамасында келесі функционалдық мүмкіндіктер орындалуы керек:

· нақты уақыт режимінде және объектінің контекстік мәзірінен сұраныс бойынша антивирустық сканерлеу;

· кесте бойынша антивирустық сканерлеу;

· қосылатын құрылғыларды вирусқа қарсы сканерлеу;

· бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;

· белсенді залалдану әрекеттерін бейтараптандыру;

· қолданбаның әрекетін және оның зиянды әрекетін анықтау және рұқсат етілмеген әрекеттерді анықтау үшін жүйедегі әрекеттерін талдау;

· желі арқылы қолжетімді қорғалған ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қол жеткізуді талдау;

· бағдарламалық қамтамасыз етудегі осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, соның ішінде жүйелік процестердің жадын қорғау;

· шифрланған, зиянды бағдарламаларды, файлдарды қалпына келтіруді қоса алғанда, емдеу кезінде зиянды бағдарламалық қамтамасыз етудің әрекеттерін кері қайтару;

· қолданбаға іске қосылған бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің ресурстарына қол жеткізуге мүмкіндік беретін жаңа қауіптерден бұлттық қорғаныс;

· RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматындағы архивтердегі файлдарды антивирустық тексеру және емдеу;

· желілік сегменттерді санаттарға бөлу мүмкіндігімен желілік пакеттік ережелерді және бағдарламаларға арналған желілік ережелерді жасауға мүмкіндік беретін кіріктірілген желілік қалқан;

· құрылғының MAC мекенжайын бұрмалау үшін ARP протоколындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;

· зиянды бағдарламалар, зиянкестер немесе біліктілігі жоқ пайдаланушылар тарапынан қорғауды өшіруді болдырмауға мүмкіндік беретін қолданба сервисін қашықтан рұқсатсыз басқарудан қорғауды, сондай-ақ құпия сөз арқылы қолданба параметрлеріне кіруді қорғауды қамтамасыз етеді;

· вирусқа қарсы қорғау бағдарламалық құралының таңдалған құрамдастарын ғана орнату;

· жоғарыда аталған барлық құрамдастарды бірыңғай басқару жүйесі арқылы орталықтандырылған басқару;

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

· файлдық кеңістікті сканерлеуді орындау кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютерлік ресурстарды пайдалануды икемді басқару;

· өткен тексеруден бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жылдамдату;

· антивирустық бағдарламаның тұтастығын тексеру;

· файлдың бақылау сомасы, аты/каталог маскасы бойынша немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктерді қосу;

· антивирустың жойылған вирус жұққан файлдарды қалпына келтіру мүмкіндігімен қорғалған қоймасының болуы;

· антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы;

· антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ ең аз мүмкіндіктер жиынтығымен графикалық интерфейстің жеңілдетілген нұсқасының болуы;

· интеграциялар бастап Windows Defender Security Center;

· болуы қолдауды Antimalware Scan Interface (AMSI);

· болуы қолдауды Windows Subsystem for Linux (WSL);

· сақтық көшірме қоймасынан нысандарды қалпына келтіруді құпия сөзбен қорғаңыз.

· ережелер мен ерекшеліктер тізімдерін XML пішіміне импорттау және экспорттау;

· интернетке қосылу лимитті болып табылған жағдайда желілік трафиктің шектеулері;

· барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді жасау үшін құрамдас

бағдарламаны табу жолында, метадеректерде, сертификатта немесе оның саусақ ізінде, бақылау сомасында, сондай-ақ бағдарламалық құрал өндірушісі қамтамасыз ететін қолданбалардың алдын ала анықталған санаттары, құрамдас қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе блоктау режимінде жұмыс істеуі керек;

· анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қолданбалардағы осалдықтарды анықтау және жабу үшін арнайы тапсырманы іске қосу;

· құрамдастарды қолдау Веб-қауіптерден қорғау, Электрондық пошта қауіптерінен қорғау, Веб-бақылау және Серверлерге арналған Windows операциялық жүйесі бар компьютерлерге арналған құрылғыларды басқару.

· тексеру тоқтатылған жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;

· тапсырманы орындау ұзақтығына шектеу қою мүмкіндігі;

· тексеру әлдеқашан орындалып жатқан болса, тексеру тапсырмаларын кезекке қою мүмкіндігі;

· жүйені қайта іске қоспай жаңарту;

· қолжетімділік құқықтарының баптаулары (оқу / жазу) портативті құрылғылар үшін (MTP), құрылғыларға қол жеткізе алатын пайдаланушыларды немесе пайдаланушылар тобын таңдаңыз, сондай-ақ құрылғыларға қол жеткізу кестесін орнатыңыз;

· мобильді құрылғыға кіруге тыйым салынған болса да, құрылғыны компьютерге USB арқылы қосу арқылы мобильді құрылғыны зарядтаңыз;

· пайдаланушылар үшін басып шығару құқықтарын теңшеңіз;

· желілерге қосылуды бақылау үшін WPA3 протоколының қолдауының болуы Wi-Fi;

· Azure WVD жүйесімен үйлесімділіктің болуы;

· операциялық жүйені қайта іске қоспай-ақ қолданбаны жаңарту мүмкіндігі;

· зиянды бағдарламаны іздеу тапсырмасы үшін процессор ресурстарын тұтынуды шектеу мүмкіндігі.

· қолданба қызметтерін сырттан басқаруға тыйым салу мүмкіндігі.

· SQL-серверлерінде, Microsoft Exchange-серверлерінде және System Center Configuration Manager-де қосымшаның жұмыс істеуі үшін сенімді аймақты жылдам конфигурациялауға арналған тексеруден және сенімді қосымшалардан алдын ала орнатылған ерекшеліктерді пайдалану мүмкіндігі;

· хаттаманы қолдау Kerberos интернетке қол жеткізу үшін прокси-сервер арқылы қосымшаның аутентификациясы үшін;

· көрсету мүмкіндігі хэш қосымшаны тексеруден шығаруға арналған файл.

Мас жұмыс станцияларына арналған антивирустық бағдарламалық қамтамасыздандыруға қойылатын талаптар

Жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары Mac операциялық жүйелердің келесі нұсқаларын басқаратын компьютерлерде жұмыс істеуі керек:

o macOS 12 - 15;

Антивирустық қорғаудың бағдарламалық жасақтамасында келесі функционалдық мүмкіндіктер орындалуы керек:

· резиденттік вирусқа қарсы мониторинг;

· қолданбаға іске қосылған бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына қол жеткізуге мүмкіндік беретін жаңа қауіптерден бұлттық қорғаныс;

· вирусқа қарсы дерекқорларды кесте бойынша автоматты түрде жаңарту;

· вирус жұққан файлдарды жоймас бұрын олардың сақтық көшірмесін жасау, қалпына келтіру мүмкіндігі үшін;

· бұрын белгісіз зиянды бағдарламаларды тануға және блоктауға мүмкіндік беретін эвристикалық анализатор;

· кіруді анықтау және алдын алу жүйесін (IDS/IPS) және кез келген түрдегі компьютерлік желілерде, соның ішінде сымсыз желілерде жұмыс істегенде ең танымал қолданбаларға арналған желілік белсенділік ережелерін пайдалана отырып, желілік шабуылдардан қорғау;

· вирусқа қарсы қорғаныс құралдарын өндірушінің беделді бұлттық қызметтерінің үкімдері негізінде зиянды бағдарламалар мен фишингтік сайттарды блоктау;

· Safari, Google браузерлері арқылы тасымалданатын желілік трафикті тексеру Chrome және Firefox (HTTP және HTTPS трафигі);

· пайдаланушының Интернет желісімен жұмысын, соның ішінде санаттарды қосуды, өңдеуді, өндіруші жасаған және динамикалық түрде жаңартып отыратын белгілі бір ресурстарға немесе ресурстар санаттарына қол жеткізуге нақты тыйым салуды немесе рұқсатты қосуды бақылау

· соңғы тексеруден бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жылдамдату;

· файлдық операцияларды тоқтату деңгейінде көрсетілген аймақтарды тексеру кезінде ерекшеліктерді орнатыңыз;

· дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде қадағалаңыз және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнатыңыз;

· зиянды бағдарламаны іздеу тапсырмаларын орындау кезінде қолданбаның процессорды пайдалануын шектеу;

· операциялық жүйе ресурстарына жүктемені азайту үшін бұлттық режимді қосу және зиянды бағдарламалық қамтамасыз ету дерекқорларының жеңіл нұсқасын пайдалану;

· сұраныс бойынша тексеру тапсырмаларын орындау кезінде тек оқуға арналған жүйе көлемін сканерлеуді өткізіп жіберу;

· қауіпті мінез-құлық үлгілерін пайдалана отырып, операциялық жүйедегі қолданба әрекеттерін талдау (BSS);

· файлдан орнатулар .pkg JAMF арқылы;

· сыртқы дискілерді қосқан кезде оларды автоматты түрде сканерлеңіз;

· клиенттік сертификаттарды қолдау;

· кіріс және шығыс электрондық пошта тіркемелерінде зиянды бағдарламалардың және басқа қауіптердің бар-жоғын тексеру;

· пайдаланушылардың компьютерге орнатылған немесе қосылған құрылғыларға қол жеткізуін басқару;

· Интернетте немесе жергілікті желіде жұмыс істеу кезінде компьютерге рұқсатсыз қосылуларды блоктау және қосымшалардың желілік белсенділігін бақылау;

· ОЖ-дағы оның файлдық, жүйелік немесе желілік белсенділігіне қатысты зиянды бағдарламалық құралдың әрекеттерін кері қайтару;

· эксплуатациялардан қорғау.

· жоғарыда аталған барлық компоненттерді бірыңғай басқару жүйесін қолдана отырып орталықтандырылған басқару.

Linux жұмыс станциялары мен серверлеріне арналған антивирустық бағдарламалық қамтамасыздандыруға қойылатын талаптар

Жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары Linux келесі нұсқалардың 32 биттік операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:

o Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

Жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары Linux 64 биттік операциялық жүйелердің келесі нұсқаларында жұмыс істейтін компьютерлерде жұмыс істеуі керек:

o AlmaLinux OS 8.6, 8.7, 8.8, 8.9.

o AlmaLinux OS 9.4, 9.5, 9.6.

o AlterOS® 2025.

o Amazon™ Linux 2023.

o Astra Linux Common Edition 2.12.

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

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

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

o Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.8).

o Astra Linux Special Edition РУСБ.10015-03 (кезекті жаңарту 7.6).

o Astra Linux Special Edition Орыс.10015-16 (1-нұсқа) (кезекті жаңарту 1.6).

o Astra Linux Special Edition РУСБ.10015-17 (кезекті жаңарту 1.7.3).

o Astra Linux Special Edition РУСБ.10015-37 (кезекті жаңарту 7.7).

o CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.

o CentOS Stream 8.

o CentOS Stream 9.

- CentOS Stream 10.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
- Debian GNU/Linux 13.0, 13.1, 13.2.
- EMIAS 1.0.
- EulerOS 2.0 SP10.
- Fedora 41.
- Kylin 10.
- Linux Mint 21.3.
- Linux Mint 22.2.
- Mostech 12 release 2021.1.
- openSUSE Leap 15.6.
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9.
- Oracle Linux 9.4, 9.5, 9.6.
- Red Hat® Enterprise Linux® 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9.
- Red Hat Enterprise Linux 9.4, 9.5, 9.6.
- Red Hat Enterprise Linux 10.0, 10.1.
- Rocky Linux 8.6, 8.7, 8.8, 8.9.
- Rocky Linux 9.4, 9.5, 9.6.
- SberLinux 8.10, 9.1, 9.5, 9.6.
- SberOS 3.4.0, 3.5.0.
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7.
- SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7.
- Ubuntu® 22.04 LTS.

- Ubuntu 24.04 LTS.
- Альт Білім беру 10.
- Альт Білім беру 11.
- Альт Жұмыс Станция 11.
- Альт Сервер 11.
- Альт БК Сервер шығарылым 10.
- Alt SP жұмыс станциясының шығарылымы 10.
- Атлант, құрастыру Alcyone, нұсқа 2022.02.
- Гослинукс 7.2.
- МОС 12 Сервер release 2021.1.
- МосОС 15.5 Arbat.
- МСВСФЕРА 9.4 АЖО.
- МСВСФЕРА 9.4 СЕРВЕР.
- ОЖ БҒМ 12 Барлық пайдаланушылар үшін (телеметриясыз және ДИТ қолдауынсыз) relea se 2021.1.
- Мәскеу мектептері үшін интерактивті панельдерге арналған OS MESH 12 (телеметриямен және DIT қолдауымен) release 2021.1.
- Мәскеу мектептері үшін компьютерлер мен ноутбуктерге арналған OS MESH 12 (телеметриямен және DIT қолдауымен) release 2021.1.
- Негізі 2.14.
- Негізі 3.0.5.
- РЕД ОС® 7.3.
- РЕД ОС 8.0.
- ШЫҚ "Кобальт" 7.9 Жұмыс станция.
- ШЫҚ "Кобальт" 7.9 Сервер.
- ШЫҚ "Хром" 12 Жұмыс станция.

- ШЫҚ "Хром" 12 Сервер.
- СинтезМ-Клиент 8.6.
- СинтезМ-Сервер 8.6.

Архитектураға арналған 64 биттік операциялық жүйелерге қолдау көрсетіледі ARM:

- Astra Linux Special Edition орыс.10152-02 (кезекті жаңарту 4.7).
- CentOS Stream 9.
- EulerOS 2.0 SP10.
- SUSE Linux Enterprise Server 15.
- Ubuntu 22.04 LTS.
- Alt SP жұмыс станциясының шығарылымы 10.
- Alt SP серверінің шығарылымы 10.
- РЕД ОС 8.0.

Антивирустық қорғаудың бағдарламалық жасақтамасында келесі функционалдық мүмкіндіктер орындалуы керек:

· резиденттік вирусқа қарсы мониторингтің;

· жаңа қауіптерден бұлттық қорғаныс, бұл қолданбаға іске қосылған бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуге мүмкіндік береді;

· SMB/NFS қолжетімді ресурстарды тексеру;

· ядро жадын тексеру мүмкіндігі;

· бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және блоктауға мүмкіндік беретін эвристикалық анализатор;

· пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу;

· мұрағаттардағы файлдарды вирусқа қарсы тексеру zip; .7z*; .7-z; .rar; .iso; .cab; .jar; . bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;

· кіріс және шығыс электрондық пошта хабарларын тексеру;

· файлдарды тексеруді оңтайландыру механизмдерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытының шегі, тексерілетін файл өлшемінің шегі, кэштеу механизмі тексерілген және тексерілгеннен кейін өзгертілмеген файлдар туралы ақпарат);

· SMB / NFS хаттамалары бойынша желілік қолжетімділігі бар жергілікті каталогтардағы файлдарды қашықтан зиянды шифрлаудан қорғау;

· тексеру кезінде файлдарды құлыптау опциясын қосу;

· күдікті және бүлінген объектілерді карантинге орналастыру;

· SAMBA деңгейіндегі файлдық операцияларды ұстап 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;

· HTML және CSV пішіміндегі есептерді экспорттау және сақтау;

· файлдық кеңістікті сканерлеуді орындау кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін ДК ресурстарын пайдалануды икемді басқару;

· залалданған объектінің көшірмесін, егер ол ақпараттық құндылықты білдірсе, талап ету бойынша объектіні ықтимал қалпына келтіру мақсатында емдеу және жою алдында резервтік қоймада сақтау;

· пайдаланушылық графикалық интерфейс арқылы басқарусыз root құқықтарды;

· жоғарыда аталған барлық құрамдастарды бірыңғай басқару жүйесі немесе веб-консоль арқылы орталықтандырылған басқару;

· құрылғы түрлері мен қосылу шиналары бойынша пайдаланушылардың компьютерге орнатылған немесе қосылған құрылғыларға қол жеткізуін басқару;

· алынбалы дискілерді тексеру;

· кіретін желілік трафиктегі желілік шабуылдарға тән әрекеттерді қадағалау;

· HTTP/HTTPS және FTP хаттамалары бойынша пайдаланушының компьютеріне түсетін трафикті, сондай-ақ веб-мекенжайлардың зиянды немесе фишингтік мекенжайларға тиесілігін белгілеу мүмкіндігін тексеру

· пайдаланушының компьютеріндегі бағдарламалардың әрекеттері туралы мәліметтер алу;

· компьютерлерде сақталатын бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу (түгендеу тапсырмасы);

· бағдарламаны іске қосқан кезде бақылау файлдарын жасаңыз;

· компьютерлерде орнатылған бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу;

· автоматты іске қосу нысандарын, жүктеу секторларын, процесс жадын және ядро жадын тексеру;

· емдеу немесе жою алдында файлдардың сақтық көшірмелерін сақтау және сақтық көшірмелерден файлдарды қалпына келтіру;

· бағдарламаның жалпы параметрлеріндегі процестердің жадын тексеруден процестердің ерекшеліктері;

· параметрді пайдаланып бағдарламалардың журналдарын тексеруді оңтайландыру SkipPlainTextFiles;

· трафикті бағдарламамен тексеруден алып тастау;

· ақпаратты сұрау және шығару, бағдарлама параметрлері мен тапсырма параметрлерін экспорттау және импорттау үшін JSON пішімін пайдаланыңыз;

· архитектураға арналған операциялық жүйелері бар құрылғылардағы қондырғылар мен жұмыстар Arm;

· қауіптер анықталған жағдайда немесе құрылғыға кіру әрекеті анықталған жағдайда пайдаланушыны ақпараттандыру режимінде жұмыс істеу;

· тыйым салынған немесе рұқсат етілген қолданбалар тізімі режимдерінде бақылау ережелерін пайдалану арқылы қорғалған құрылғыларда қолданбалардың іске қосылуын басқару мүмкіндігі;

· жаңарту кезінде қолданбаны автоматты түрде қайта іске қосыңыз;

· процессор ресурстарын пайдалануға шектеуді орнату мүмкіндігі;

· орнатқаннан кейін қолданбаны іске қосқан кезде қорғаныс құрамдастарын және тексеру тапсырмаларын автоматты түрде өшіру мүмкіндігі;

· графикалық пайдаланушылық интерфейстегі құрамдастардың және тапсырмалардың жұмысы туралы пайдаланушыны хабардар ету;

· процестердің жадын оларды тоқтатпай оқу мүмкіндігі (Linux ядролары 3.4 нұсқасынан бастап);

· пайдаланушылардың веб-ресурстарға қолжетімділігін басқару мүмкіндігі;

· қорғалатын құрылғыларда қосымшалардың іске қосылуын басқару мүмкіндігі;

· қосымшаның жеке жұмысының тұрақтылығын бақылау функциясы;

· объектілерді тексеруден алып тастауды теңшеу мүмкіндігімен эксплуатациядан қорғау;

· қосылған құрылғылар сенімді болатын құрылғыларды басқару пайдаланушыларының немесе пайдаланушылар топтарының тізімін теңшеу мүмкіндігі;

· деректерді сақтау құрылғыларына тек оқуға арналған рұқсаттарға рұқсат беру мүмкіндігі;

· прокси серверді пайдалану кезінде қолданбаның жеке құрамдастары үшін ерекшеліктерді конфигурациялау мүмкіндігі;

· трафикті ұстап қалудан ерекшеліктерді теңшеу мүмкіндігі;

· дерекқорлар журналдарының файлдарын тексеруден уақытша алып тастау мүмкіндігі;

· қолданбаға қолданылатын саясаттар мен тапсырмалардағы ерекшеліктер тізімдерін экспорттау және импорттау мүмкіндігі;

· батарея қуатымен жұмыс істейтін құрылғыда жоспарланған тапсырмалардың іске қосылуын болдырмауды конфигурациялау мүмкіндігі;

· пәрмен жолында қолданба функцияларын, олардың күйлері (пайдаланылған немесе пайдаланылмаған) және осы қолданба функциялары жүзеге асырылатын Linux технологиялары туралы ақпаратты тізімдеу мүмкіндігі;

· типті шабуылдардан қорғану мүмкіндігі BadUSB;

· пәрмен жолында және графикалық интерфейсте құрылғыдағы қолданыстағы саясат және саясат профильдері туралы ақпаратты көрсету мүмкіндігі.

Мобильді құрылғылардың антивирустық қорғанысының бағдарламалық құралдарына қойылатын талаптар

Смартфондарды антивирустық қорғауға арналған бағдарламалық жасақтама келесі мобильді ОЖ-нің басқаруымен жұмыс істеуі керек:

o Android 5.0 және одан жоғары (қоса алғанда Android 12L, қоспағанда Go Edition);

o iOS 15 және одан жоғары немесе iPadOS 15 және одан жоғары;

ОЖ-ға арналған смартфондардың антивирустық қорғаныс бағдарламалық жасақтамасында Android келесі функционалдық мүмкіндіктерді жүзеге асыру қажет:

· вирусқа қарсы қорғаныс құралдарын өндірушінің бұлтқа негізделген беделді қызметін пайдалана отырып, қосымша тексеру деңгейімен смартфонның файлдық жүйесін тұрақты антивирустық қорғау;

· құрылғының файлдық жүйесін сұраныс бойынша және кесте бойынша тексеру;

· орнатылатын қосымшаларды лезде тексеру

· вирусқа қарсы қорғаныс құралдарын өндірушінің беделді бұлттық қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды блоктау;

· залалданған объектілерді оқшаулауға арналған қойманың болуы;

· кесте бойынша зиянды бағдарламаларды іздеу және қауіпті нысандарды жою кезінде пайдаланылатын антивирустық дерекқорларды жаңарту;

· көрсетілген қолданбалардың, соның ішінде алдын ала анықталған қолданба санаттары арқылы іске қосылуын блоктау;

· рұқсат етілген қолданбалардың ақ тізімдерін қолдау;

· қолданбаларды іске қосуды басқару бөлігі ретінде жүйелік қолданбаларды құлыптау;

· командаларды жіберу және push сервис арқылы хабарламалар Firebase Cloud Messaging (FCM);

· бұғаттау wi-fi және bluetooth модульдер, сондай-ақ мобильді құрылғының камерасын пайдалану;

· қосылу параметрлерін көрсетіңіз wi-fi желілерге;

· орнатуға міндетті қосымшаларды көрсету;

· мобильді құрылғыны құлыптау, деректерді жою, жою деректердің жұмыс әрекетіне байланысты, құрылғының орналасқан жерінің координаттарын алу, зауыттық параметрлерге қашықтан оралу (factory reset);

· мобильді құрылғының корпоративтік саясаттарға сәйкестігі тексерілетін ережелер тізімін жасау, сәйкессіздіктер анықталған жағдайда құрылғыны автоматты түрде құлыптау, деректерді жою, корпоративтік қолданбаларды іске қосуға тыйым салу мүмкіндігімен;

· Samsung KNOX1 және KNOX2 технологияларын қолдау;

· қолданбаларды басқару ережелерін жасау кезінде қолданбалардың рұқсат етілген нұсқаларын көрсетіңіз Androidқұрылғылар.

ОЖ-ға арналған смартфондарды қорғаудың бағдарламалық құралында Apple iOS келесі функционалдық мүмкіндіктерді жүзеге асыру қажет:

· параметрлерді қашықтан баптау iOS Топтық саясаттарды пайдаланатын MDM құрылғылары;

· деректерді блоктау және жою пәрменін жіберу;

· мобильді құрылғылардың топтық қауіпсіздік саясаттарын жасаңыз;

· Exchange протоколы арқылы қосылған құрылғылардың конфигурациялық параметрлерін қашықтан конфигурациялау ActiveSync\ iOS MDM;

· пайдаланушылардың мобильді құрылғыларының жұмысы туралы есептер мен статистиканы алу;

· пайдаланған кезде антивирустық қорғаныс құралдарын өндірушінің беделді бұлттық қызметтерінің үкімдері негізінде зиянды бағдарламалар мен фишингтік сайттарды бұғаттау supervised mode;

· бірыңғай басқару консолі арқылы орталықтандырылған басқару;

· құрылғының жергілікті қолданбаларын пайдалануға болатын-болмайтынын басқаруға мүмкіндік беретін құрамдас бөліктің болуы, мысалы iTunes, Safari немесе Game Center, басқарылатын құрылғыда.

· Bluetooth параметрлерін өзгертуге тыйым салу iOS MDMқұрылғылар

Windows ОЖ базасында орталықтандырылған басқарудың, мониторингілеудің және жаңартудың бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқарудың, бақылаудың және жаңартудың бағдарламалық құралдары операциялық жүйелердің келесі нұсқаларын басқаратын компьютерлерде жұмыс істеуі керек:

o Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.

o Windows Server 2016 Standard/Datacenter/Essentials/Server Core (нұсқалары қондырғылар) (LTSB) 64-разрядты.

o Windows Server 2019 Standard/Datacenter/Core 64-разрядная.

o Windows Server 2022 Standard/Datacenter/Core 64-разрядная.

- Windows Server 2025 Standard/Datacenter/Core 64-разрядная.
- Windows Storage Server 2019 64 биттік болып табылады.

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

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- Microsoft Hyper-V Server 2019 64-разрядты.
- Microsoft Hyper-V Server 2022 64-разрядты.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.x.

Орталықтандырылған басқарудың, бақылаудың және жаңартудың бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі керек:

- Microsoft SQL Server 2016 (барлық басылымдар) 64 бит. 2016 (барлық басылымдар) 64 бит.
- Microsoft SQL Server 2017 (барлық басылымдар) үшін Windows/Linux 64-разрядты.
- Microsoft SQL Server 2019 (барлық басылымдар) үшін Windows/Linux 64 бит (қосымша қадамдар қажет).
- Microsoft SQL Server 2022 (барлық басылымдар) үшін Windows/Linux 64-разрядты.
- mySQL 5.7 қауымдастығы 32 биттік/64 биттік.
- mySQL 8.0 қауымдастығы 32 биттік/64 биттік.
- MariaDB 10.5 (10.5.17 және одан жоғары нұсқасы) 32 биттік/64 биттік.
- MariaDB Galera Cluster 10.3 32 биттік/64 биттік сақтау ішкі жүйесімен InnoDB.
- PostGresql 13.x 64 биттік.
- PostGresql 14.x 64 биттік.
- PostGresql 15.x 64 биттік.

o Postgres Pro 13.x Windows/Linux 64 биттік нұсқасы.

o Postgres Pro 14.x Windows/Linux 64 биттік нұсқасы.

Антивирустық қорғаудың бағдарламалық жасақтамасында келесі функционалдық мүмкіндіктер орындалуы керек:

· қорғалатын түйіндердің санына байланысты орталықтандырылған басқару, бақылау және жаңарту қондырғысының архитектурасын таңдау;

· ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы мәліметтерді алу үшін Active Directory-ден ақпаратты оқу;

· анықталған компьютерлерді тасымалдау ережелерінің параметрлері ір-мекенжайы, ОЖ типі, OU AD мекенжайында болуы;

· желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтары бойынша автоматты түрде бөлу; Бағдарламалық жасақтаманы тасымалдау ережелерін конфигурациялау мүмкіндігі ір-мекенжайы, ОЖ типі, OU AD мекенжайында болуы;

· антивирустық қорғау бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою;

· орталықтандырылған баптау, әкімшілендіру;

· қорғау құралдарының жұмысы бойынша есептерді және статистикалық ақпаратты қарау;

· басқару орталығының құралдарымен үйлеспейтін қосымшаларды орталықтан жою (қолмен және автоматты түрде);

· саясаттар мен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;

· вирусқа қарсы агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін - RPC, GPO, басқару жүйесінің құралдары, жергілікті орнату үшін – автономды орнату бумасын жасау мүмкіндігі;

· пайдаланушы жүйеге кірген есептік жазбаға байланысты антивирустық шешімнің параметрлерін жоққа шығаратын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулары ағымдағы IPv4-мекен-жайлар, сондай-ақ компьютер қандай ОС-да немесе қандай қауіпсіздік тобында орналасқан;

· қайта бөлу орын алатын триггерлер иерархиялары;

· жүктелген жаңартуларды клиенттік машиналарға таратпас бұрын орталықтандырылған басқару бағдарламалық жасақтамасының құралдарымен тексеру;

· жаңартуларды пайдаланушылардың жұмыс орындарына оларды алғаннан кейін бірден жеткізу;

· желіде виртуалды машиналарды тану және егер бұл машиналар бір физикалық серверде орналасқан болса, олардың арасында іске қосылған тапсырмалардың жүктеме балансын бөлу;

· әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігі бар көп деңгейлі басқару жүйесін құру;

· еркін деңгейдегі әкімшілендіру серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтан басқару мүмкіндігі;

· қолдау мульти-жалдаушылықтар (multi-tenancy) басқару серверлері үшін;

· бағдарламалық жасақтама құралдарын және антивирустық дерекқорларды байланыс арналары арқылы да, машиналық сақтау құралдары арқылы да әртүрлі көздерден жаңарту;

· антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне басқару сервері арқылы қол жетімділік;

· клиенттік компьютерлерге лицензияны автоматты түрде тарату;

· пайдаланушылардың компьютерлерінде орнатылған БҚ мен жабдықтарды түгендеу;

· орнатылған антивирустық қорғаныс қосымшаларының жұмысындағы оқиғалар туралы хабарлау механизмінің болуы және олар туралы пошта хабарламаларын таратуды конфигурациялау;

· мобильді құрылғыларды сервер арқылы басқару функциясы iOS MDM;

· тапсырылған оқиғалар туралы SMS-хабарламалар жіберу;

· басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату;

· ұйымның кез келген компьютерінің басқару жүйесіне желілік жүктемені азайту үшін жаңарту релесі орталығының нұсқаулары;

· ұйымның кез келген компьютеріне антивирустық агенттердің оқиғаларды бағыттау орталығының, клиенттік компьютерлердің таңдалған тобының, орталықтандырылған басқару серверінің басқару жүйесіне желілік жүктемені азайту жөніндегі нұсқаулары;

· вирусқа қарсы қорғау оқиғалары, түгендеу деректері, орнатылған бағдарламаларды лицензиялау деректері бойынша графикалық есептерді құрастыру;

· болуы алдын ала бапталған жүйенің жұмысы туралы стандартты есептер;

· есептерді PDF және XML файл пішімдеріне экспорттау;

· вирусқа қарсы бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік қоймалар мен карантиндер объектілерін орталықтандырылған басқару;

· басқару серверінде аутентификация үшін ішкі тіркелгілерді жасау;

· басқару жүйесінің кіріктірілген құралдарымен басқару жүйесінің резервтік көшірмесін жасау;

· қолдау Windows Failover Clustering;

· қолдау интеграциялар бастап Windows сервиспен Certificate Authority;

· пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы;

· өзіне-өзі қызмет көрсету порталы мобильді құрылғыға басқару агентін орнату, мобильді құрылғыларды қарау, блоктау пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобильді құрылғысындағы деректерді жою мақсатында пайдаланушыларды қосу мүмкіндігін қамтамасыз етуі керек;

· вирустық індеттердің пайда болуын бақылау жүйесінің болуы;

· Microsoft Azure және Google бұлттық инфрақұрылымындағы орнатулар Cloud;

· БҚ интеграциялары OpenAPI;

· WEB консольді пайдалана отырып антивирустық қорғанысты басқару;

· ОЖ орналастыруды басқару мүмкіндігі Windows басқару консолі арқылы;

· болуы алдын ала бапталған орталықтандырылған басқару құралдарын пайдаланушылардың рөлдері;

· пайдаланушы тіркелгілерімен байланыстыру үшін арнайы көрсетілген өкілеттіктер жиынтығымен арнайы рөлдерді жасау мүмкіндігі іске асырылуы керек;

· RDP арқылы немесе басқару консолінен стандартты құралдармен қосылу мүмкіндігі;

· жұмыс үстеліне бірлесіп қосылу мүмкіндігінің болуы Windows (Windows Desktop Shar ing);

· пайдаланушыға қашықтан қосылуға рұқсат беру туралы сұрау салынуы керек;

· ОЖ кескіндерімен жұмыс істеуге арналған құралдардың болуы: Физикалық немесе виртуалды машинаның негізінде мақсатты ОЖ кескінін құру, кескінді әкімші таңдаған компьютерлерге, соның ішінде "жалаң металға" орнату (bare metal);

· бұрын жасалған кескінге драйверлер жиынтығын қосу мүмкіндігі қамтамасыз етілуі керек;

· ОЖ орнатқаннан кейін сценарийлерді іске қосу немесе қосымша бағдарламалық жасақтаманы автоматты түрде орнату мүмкіндігі;

· операциялық жүйенің кескінін дистрибутивтерден (WIM) импорттау мүмкіндігі

· лицензияны пайдаланудың бұзылғаны немесе лицензияның қолданылу мерзімінен асып кеткені туралы әкімшіге хабарлау мүмкіндігімен компьютерде орнатылған бөгде БҚ лицензияларын бақылау жүйесінің болуы;

· бөгде қосымшаларға (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) арналған орнату бумаларын автоматты түрде құру және осы қосымшалар бумаларын компьютерлерге орталықтандырылған түрде автоматты түрде орнату;

· деректерді шифрлауды басқарудың функционалдығын қолдау;

· SIEM жүйелерімен интеграциялау және оқиғаларды форматта жіберу мүмкіндігі syslog немесе CEF\ LEEF

· әкімшілік консоліне рұқсатсыз кіру қаупін азайту үшін екі сатылы растау;

· пайдаланушы тіркелгісінің параметрлерін өзгерткеннен кейін қосымша аутентификацияны пайдалану.

· IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрау мүмкіндігі.

· Microsoft басқаратын пайдаланушылар компьютерлері мен серверлерінде орнатылған қолданбалар мен операциялық жүйедегі осалдықтарды автоматтандырылған іздеу және жабу Windows;

· әкімшілік серверді қолжетімділігі жоғары жүйе ретінде орналастыру мүмкіндігі;

· жаңартуларды орнату және оқшауланған желідегі үшінші тарап бағдарламаларының (Microsoft бағдарламаларынан басқа) осалдықтарын жабу мүмкіндігі.

· Windows және Linux негізіндегі клиенттік құрылғыларды қашықтан диагностикалау (іздерді, оқиғалар журналдарын, қоқыстарды алу, қолданбаларды тоқтату және іске қосу);

· Linux операциялық жүйесі бар басқарылатын құрылғылардағы тіркелгілердің жергілікті әкімшісінің құқықтарын қайтарып алу мүмкіндігі;

· Linux операциялық жүйесі бар басқарылатын құрылғыларда жергілікті тіркелгі құпия сөзін өзгерту мүмкіндігі.

Linux ОЖ базасында орталықтандырылған басқарудың, мониторингілеудің және жаңартудың бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқарудың, бақылаудың және жаңартудың бағдарламалық құралдары операциялық жүйелердің келесі нұсқаларын басқаратын компьютерлерде жұмыс істеуі керек:

- Debian GNU/Linux 12 (Bookworm) 64-разрядты.
- Debian GNU/Linux 13 (Trixie) 64-разрядты.
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядты.
- Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядты.
- CentOS Stream 9 64 биттік болып табылады.
- CentOS Stream 10 64 биттік.
- Red Hat Enterprise Linux Server 7.x 64-разрядты.
- Red Hat Enterprise Linux Server 8.x 64-разрядты.
- Red Hat Enterprise Linux Server 9.x 64-разрядты.
- Red Hat Enterprise Linux Server 10.x 64-разрядты.
- SUSE Linux Enterprise Server 12 (барлық қызмет бумалары) 64 биттік.
- SUSE Linux Enterprise Server 15 (барлық қызмет бумалары) 64 биттік.
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.6) 64 биттік.
- Astra Linux Special Edition RUSB.10015-01 (келесі жаңарту 1.7) 64 биттік.
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.8) 64 биттік.
- Astra Linux Special Edition RUSB.10015-16 (1-нұсқа) (келесі жаңарту 1.6) 64 биттік.
- Astra Linux Special Edition RUSB.10015-17 (келесі жаңарту 1.7.3) 64 биттік.
- Astra Linux Special Edition RUSB.10015-03 (кезекті жаңарту 7.6) 64 биттік.
- Astra Linux Special Edition RUSB.10015-37 (кезекті жаңарту 7.7) 64 биттік.

- Astra Linux Common Edition (кезекті жаңарту 2.12) 64 биттік.
- Alt SP сервері 10 64 биттік.
- Alt SP жұмыс станциясы 10 64 биттік.
- Oracle Linux 7 64 биттік болып табылады.
- Oracle Linux 8 64 биттік болып табылады.
- Oracle Linux 9 64 биттік болып табылады.
- Platform V SberLinux OS Server (SLO) 8.10.1 64-разрядты.
- Platform V SberLinux OS Server (SLO) 9.5.1 64-разрядты.
- Platform V SberLinux OS Server (SLO) 9.6 64-разрядты.
- РЕД ОС 7.3 Сервер 64-разрядты.
- РЕД ОС 7.3 Сертификатталған нұсқасы 64-разрядты.
- РЕД ОС 8 64-разрядты.
- "КОБАЛЬТ" ШЫҚ 7.9 64-разрядты.
- М ОЖ (Moscow Electronic School) 12 Сервер 64-разрядты.
- Mostech Server 64-разрядты.
- МосОС 15.5 Arbat 64-разрядты.

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

- VMware vSphere 6.7.0.
- VMware vSphere 7.0.3.
- Microsoft Hyper-V Server 2019 64-разрядты.
- Microsoft Hyper-V Server 2022 64-разрядты.
- Citrix XenServer 7.x.
- Citrix XenServer 8.2.
- Parallels Desktop 18.

- Oracle VM VirtualBox 7.0.12.
- Kernel-based Virtual Machine (барлығы қолдау көрсетілетіндер ОЖ Linux).

Орталықтандырылған басқарудың, бақылаудың және жаңартудың бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі керек:

- mySQL 5.7 қауымдастығы 32 биттік/64 биттік.
- mySQL Standard Edition 8.0 (8.0.20 және одан жоғары нұсқасы) 32 биттік/64 биттік.
- mySQL Enterprise Edition 8.0 (8.0.20 және одан жоғары нұсқасы) 32 биттік/64 биттік.
- MySQL Standard Edition 8.4 32-разрядты/64-разрядты.
- MySQL Enterprise Edition 8.4 32-разрядты/64-разрядты.
- MariaDB 10.1 (құрастыру 10.1.30 және одан жоғары) 32 бит/64 бит.
- MariaDB 10.3 (құрастыру 10.3.22 және одан жоғары) 32 бит/64 бит.
- MariaDB 10.4 (10.4.20 және одан жоғары нұсқасы) 32 биттік/64 биттік.
- MariaDB 10.5 (10.5.27 және одан жоғары нұсқасы) 32 биттік/64 биттік.
- MariaDB 10.6 (10.6.20 және одан жоғары нұсқасы) 32 биттік/64 биттік.
- MariaDB 10.11 (10.11.10 және одан жоғары құрастыру) 32 бит/64 бит.
- MariaDB Galera Кластер 10.3 32 биттік/64 биттік сақтау ішкі жүйесімен InnoDB.
- PostgreSQL 13.x 64-разрядты.
- PostgreSQL 14.x 64-разрядты.
- PostgreSQL 15.x 64-разрядты.
- PostgreSQL 15.x 64-разрядты (кластер Corosync/Pacemaker).
- PostgreSQL 16.x 64-разрядты.
- PostgreSQL 17 64-разрядты.
- PostgreSQL 18 64-разрядты.
- Postgres Pro 13.x (барлық басылымдар) 64 биттік.
- Postgres Pro 14.x (барлық басылымдар) 64 биттік.

- Postgres Pro 15.x (барлық басылымдар) 64 биттік.
- Postgres Pro 15.x 64-разрядты (кластер Corosync/Pacemaker).
- Postgres Pro 16.x (барлық басылымдар) 64 биттік.
- Postgres Pro 16.x Enterprise 64-разрядты (кластер Built-in High Availability).
- Postgres Pro 17 (барлық шығарылымдар) 64 биттік.
- Postgres Pro 17 Enterprise 64-разрядты (кластер Built-in High Availability).
- Postgres Pro 18 (барлық шығарылымдар) 64 биттік.
- Postgres Pro 18 Enterprise 64-разрядты (кластер Built-in High Availability).
- Platform V Pangolin 6.5.1 64-разрядты.
- Platform V Pangolin 6.5.1 64-разрядты (кластер Built-in High Availability).
- Jatoba 4 64-разрядты.
- Jatoba 5 64-разрядты.
- Tantor SE 1C 64-разрядты.

Антивирустық қорғаудың бағдарламалық жасақтамасында келесі функционалдық мүмкіндіктер орындалуы керек:

· антивирустық қорғау бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою;

· орталықтандырылған баптау, әкімшілендіру;

· қорғау құралдарының жұмысы бойынша есептерді және статистикалық ақпаратты қарау;

· саясаттар мен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;

· қайта бөлу орын алатын триггерлер иерархиялары;

· жаңартуларды пайдаланушылардың жұмыс орындарына оларды алғаннан кейін бірден жеткізу;

· желіде виртуалды машиналарды тану және егер бұл машиналар бір физикалық серверде орналасқан болса, олардың арасында іске қосылған тапсырмалардың жүктеме балансын бөлу;

· әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігі бар көп деңгейлі басқару жүйесін құру;

· еркін деңгейдегі әкімшілендіру серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтан басқару мүмкіндігі;

· қолдау мульти-жалдаушылықтар (multi-tenancy) басқару серверлері үшін;

· бағдарламалық жасақтама құралдарын және антивирустық дерекқорларды байланыс арналары арқылы да, машиналық сақтау құралдары арқылы да әртүрлі көздерден жаңарту;

· антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне басқару сервері арқылы қол жетімділік;

· клиенттік компьютерлерге лицензияны автоматты түрде тарату;

· орнатылған антивирустық қорғаныс қосымшаларының жұмысындағы оқиғалар туралы хабарлау механизмінің болуы және олар туралы пошта хабарламаларын таратуды конфигурациялау;

· вирусқа қарсы қорғау оқиғалары, орнатылған бағдарламаларды лицензиялау деректері бойынша графикалық есептерді құру;

· болуы алдын ала бапталған жүйенің жұмысы туралы стандартты есептер;

· есептерді PDF және XML файл пішімдеріне экспорттау;

· вирусқа қарсы бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік қоймалар мен карантиндер объектілерін орталықтандырылған басқару;

· басқару серверінде аутентификация үшін ішкі тіркелгілерді жасау;

· әкімшілік консоліне рұқсатсыз кіру қаупін азайту үшін екі сатылы растау;

· басқару жүйесінің кіріктірілген құралдарымен басқару жүйесінің резервтік көшірмесін жасау;

· вирустық індеттердің пайда болуын бақылау жүйесінің болуы;

· WEB консольді пайдалана отырып антивирустық қорғанысты басқару;

· әкімшілік серверге жүктемені азайту және корпоративтік желідегі деректер трафигін оңтайландыру үшін антивирустық дерекқорларды және бағдарламалық модульдерді әкімшілік сервер арқылы да, тарату нүктелері арқылы да басқарылатын құрылғыларда жаңарту және тарату;

· жаңартуларды тексеру тапсырмасы арқылы бұл жаңартуларды басқарылатын құрылғыларға орнатпас бұрын жүктелетін жаңартулардың денсаулығы мен қателіктерін тексеріңіз;

· антивирустық мәліметтер базасын және бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары функциясын қолданыңыз;

· орталықтандырылған басқару серверлері арасында шифрлау кілттерін тасымалдау мүмкіндігі;

· негізгі сервер ретінде әрекет етіңіз және Linux немесе Windows операциялық жүйелері бар серверлерді құл ретінде басқарыңыз;

· оқиғалар үлгілерін экспорттау және импорттау мүмкіндігі;

· оқиғаларды SIEM жүйесіне CEF немесе LEEF пішімінде экспорттау мүмкіндігі;

· мобильді құрылғыларды басқару мүмкіндігі қосулы Android және iOS;

· басқарылатын құрылғыларға орнатылған бағдарламалар туралы ақпарат алу;

· Microsoft басқаратын пайдаланушылар компьютерлері мен серверлерінде орнатылған қолданбалар мен операциялық жүйедегі осалдықтарды автоматтандырылған іздеу және жабу Windows;

· Microsoft Active Directory домен контроллері арқылы құрылғыларды іздеу мүмкіндігі және Samba;

· Windows ОЖ басқаруындағы әкімшілендіру серверінен Linux ОЖ басқаруындағы әкімшілендіру серверіне деректерді автоматтандырылған тасымалдау мүмкіндігі;

· басқарылатын құрылғыларды қашықтықтан диагностикалау мүмкіндігі;

· кластерлік технологияны қолдау;

· басқарылатын құрылғылардан үйлесімсіз БҚ орталықтандырылған жою мүмкіндігі;

· басқарылатын құрылғыларды орталықтан қайта жүктеу мүмкіндігі;

· құрылғының орналасқан жеріне байланысты бірдей немесе әртүрлі орталықтандырылған басқару серверлеріне қосылу үшін Linux құрылғылары бар желіден тыс пайдаланушылар үшін қосылым профильдерін орнату мүмкіндігі;

· домен контроллерлерін қолдау FreeIPA және ALD Pro;

· бағдарламалық жасақтаманың домендік аутентификациясын қолдау Kerberos (бірыңғай кіру технологиясы, оның ішінде сертификаттар негізінде).

Вирусқа қарсы дерекқорларды жаңартуға қойылатын талаптар

Жаңартылатын вирусқа қарсы дерекқорлар мынадай функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс:

· күнтізбелік тәулік ішінде кемінде 24 рет вирусқа қарсы дерекқорларды жаңарту қағидаларын жасау;

· жаңарту жолдарының көптігі, соның ішінде – байланыс арналары арқылы және иеліктен шығарылған электрондық ақпарат тасымалдағыштары арқылы;

· электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру.

Пайдалану құжаттамасына қойылатын талаптар

· Вирусқа қарсы құралдармен бірге жеткізілетін құжаттамада тиісті антивирустық қорғаныс құралын орнату, күйге келтіру және пайдалану процесі егжей-тегжейлі сипатталуы керек.

Техникалық қолдауға қойылатын талаптар

Вирусқа қарсы бағдарламалық қамтамасыз етуді техникалық қолдау қажет:

· Оны орыс тілінде антивирустық қорғаныс құралдарын өндірушінің және оның серіктестерінің сертификатталған мамандары Қазақстан Республикасының барлық аумағында электрондық пошта және Интернет арқылы ұсынады.

Web-антивирустық шешімді өндірушінің веб-сайты орыс тілінде болуы керек, антивирустық шешімді техникалық қамтамасыз етуге арналған арнайы бөлім, жаңартылған білім қоры, сондай-ақ форум болуы керек пайдаланушы

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	Сарсеков Азиз Даниярович
Қол қойылған күні	13.11.2026

Құжат «Самұрық-Қазына» АҚ сатып алу веб-порталымен құрылған
Документ сформирован веб-порталом закупок АО «Самрук-Қазына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1271455
способом Запрос ценовых предложений

Лот № (418 У, 4583627) Услуги по продлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Ауыл Телеком"
Организатор: "Дирекция "Телеком Комплект" - филиал Акционерного общества "Казахтелеком"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	418 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.Алматы
Условия поставки	-
Срок поставки	С даты подписания договора в течение 10 рабочих дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

В рамках всей организации должны использоваться единые антивирусные средства, независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие ПК, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ и сетевых атак, и обеспечивать возможность их включения в единую систему антивирусной защиты.

Наименование продлеваемой лицензии: Kaspersky Endpoint Security for Business Advanced

Номер текущего лицензионного соглашения: 1FF0-251120-104157-833-1648

Количество лицензий для защиты рабочих станций и файловых: 100

Срок действия лицензии: 12 календарных месяцев

Срок действия технической поддержки: не менее 1 (один) года

Тип лицензии: корпоративная (1 ключ на 100 рабочих станций).

Требования к потенциальному поставщику:

В целях исключения поставки контрафактного программного обеспечения потенциальный поставщик должен предоставить письмо от компании производителя подтверждающего легальное происхождение программного обеспечения.

Коробочная редакция приниматься не будет.

Общие требования

Антивирусные средства должны включать:

» программные средства антивирусной защиты для рабочих станций Windows;

» программные средства антивирусной защиты для файловых серверов Windows;

» программные средства антивирусной защиты для рабочих станций Mac;

» программные средства антивирусной защиты для рабочих станций и серверов Linux;

» программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);

» 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/Enterprise multi-session;

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

o Windows 11 для Arm64 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;

· формировать область защиты для функции защиты папок общего доступа от внешнего шифрования;

· 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 МТР 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;

· 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;

· установки ограничение длительности выполнения задачи;

· возможность ставить задачи проверки в очередь, если проверка уже выполняется;

· обновление без перезагрузки системы;

· настроить доступ пользователей к мобильным устройствам в приложении Android Debug Bridge (ADB);

· заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;

· настроить права печати для пользователей;

· наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;

· наличие совместимости с Azure WVD;

· настроить доступ пользователей к мобильным устройствам в приложении iTunes;

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

· полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;

· восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;

· поддержка двухфакторной аутентификации при полнодисковом шифровании;

· шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);

· наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;

· шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;

· возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)

· возможность создавать служебную учетную запись агента аутентификации при шифровании диска;

· поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании;

· возможность настроить исключения и ограничить доступ ко всем Bluetooth-устройствам кроме устройств ввода;

· возможность обновления приложения без перезагрузки операционной системы;

· возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО;

· возможность запретить внешнее управление службами приложения;

· возможность выбирать предустановленные исключения из проверки и доверенные приложения;

· возможность задать разрешение отдельному пользователю на экспорт настроек в конфигурационный файл;

· возможность мониторинга и отзыва временных паролей на доступ к приложению, позволяющий сохранять историю паролей (до 30 дней) и контролировать статус (Активен, Истек, Отозван);

· возможность разрывать подключение к веб-ресурсам, запрещенными правилами Веб-Контроля, сразу после применения политики;

· возможность настраивать разные наборы компонентов для разных типов операционных систем в инсталляционном пакете;

· возможность выбирать предустановленные исключения из проверки и доверенные приложения;

· возможность блокировать сетевые соединения по устаревшему протоколу TLS 1.0;

· поддержка протокола Kerberos для аутентификации приложения через прокси-сервер для доступа в интернет;

· возможность указывать хеш файла для исключения приложения из проверки.

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 Web Server 2008 R2 Service Pack 1 и выше;

o Windows Server 2012 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);

o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);

o Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);

o Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);

o Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core).

o Windows Server 2025 Standard / Datacenter.

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;

· 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;

· создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же 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;

· запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;

· поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.

· 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;

· обновление без перезагрузки системы;

· настройки прав доступа (чтение / запись) для портативных устройств (MTP), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам;

· заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;

· настроить права печати для пользователей;

· наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;

· наличие совместимости с Azure WVD;

· возможность обновления приложения без перезагрузки операционной системы;

· возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО.

· возможность запретить внешнее управление службами приложения.

· возможность использования предустановленных исключений из проверки и доверенных приложений, предназначенных для быстрой настройки доверенной зоны для работы приложения на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager;

· поддержка протокола Kerberos для аутентификации приложения через прокси-сервер для доступа в интернет;

· возможность указывать хеш файла для исключения приложения из проверки.

Требования к программным средствам антивирусной защиты для рабочих станций Mac

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

o macOS 12 - 15;

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

· резидентный антивирусный мониторинг;

· облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

· автоматическое обновление антивирусных баз по расписанию;

· резервное копирование зараженных файлов перед их удалением, для возможности восстановления;

· эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;

· защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;

· блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;

· проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);

· контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем

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

· задавать исключения при проверке указанных областей на уровне перехватов файловых операций;

· автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены;

· ограничивать загрузку процессора приложением при выполнении задач поиска вредоносного ПО;

· включения облачного режима и использования облегченной версии баз вредоносного ПО, для снижения нагрузки на ресурсы операционной системы;

· пропускать сканирование системного тома, доступного только для чтения, во время выполнения задач проверки по требованию;

· анализа активности приложений в операционной системе с использованием шаблонов опасного поведения (BSS);

· установки из файла .pkg через JAMF;

· автоматического сканирования внешних дисков при их подключении;

· поддержки клиентских сертификатов;

· проверки вложений входящих и исходящих сообщений электронной почты на наличие в них вредоносного ПО и других угроз;

· управления доступом пользователей к установленным или подключенным к компьютеру устройствам;

· блокировки несанкционированных подключений к компьютеру во время работы в интернет или локальной сети и контроль сетевой активности приложений;

· откат действий вредоносного программного обеспечения, связанных с его файловой, системной или сетевой активностью в ОС;

· защита от эксплойтов.

· централизованного управления всеми вышеуказанными компонентами с помощью единой системы управления.

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 Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

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

- AlmaLinux OS 8.6, 8.7, 8.8, 8.9.
- AlmaLinux OS 9.4, 9.5, 9.6.
- AlterOS® 2025.
- Amazon™ Linux 2023.
- Astra Linux Common Edition 2.12.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).
- Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6).
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3).
- Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).
- CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- CentOS Stream 8.
- CentOS Stream 9.
- CentOS Stream 10.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
- Debian GNU/Linux 13.0, 13.1, 13.2.
- EMIAS 1.0.
- EulerOS 2.0 SP10.
- Fedora 41.

- Kylin 10.
- Linux Mint 21.3.
- Linux Mint 22.2.
- Mostech 12 release 2021.1.
- openSUSE Leap 15.6.
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9.
- Oracle Linux 9.4, 9.5, 9.6.
- Red Hat® Enterprise Linux® 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9.
- Red Hat Enterprise Linux 9.4, 9.5, 9.6.
- Red Hat Enterprise Linux 10.0, 10.1.
- Rocky Linux 8.6, 8.7, 8.8, 8.9.
- Rocky Linux 9.4, 9.5, 9.6.
- SberLinux 8.10, 9.1, 9.5, 9.6.
- SberOS 3.4.0, 3.5.0.
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7.
- SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7.
- Ubuntu® 22.04 LTS.
- Ubuntu 24.04 LTS.
- Альт Образование 10.
- Альт Образование 11.
- Альт Рабочая Станция 11.
- Альт Сервер 11.
- Альт СП Сервер релиз 10.

- Альт СП Рабочая Станция релиз 10.
- Атлант, сборка Alcyone, версия 2022.02.
- Гослинукс 7.2.
- МОС 12 Сервер release 2021.1.
- МосОС 15.5 Arbat.
- МСВСФЕРА 9.4 АРМ.
- МСВСФЕРА 9.4 СЕРВЕР.
- ОС МЭШ 12 Для всех пользователей (без телеметрии и без поддержки ДИТ) release 2021.1.
- ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ) release 2021.1.
- ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ) release 2021.1.
- ОСнова 2.14.
- ОСнова 3.0.5.
- РЕД ОС® 7.3.
- РЕД ОС 8.0.
- РОСА "Кобальт" 7.9 Рабочая станция.
- РОСА "Кобальт" 7.9 Сервер.
- РОСА "Хром" 12 Рабочая станция.
- РОСА "Хром" 12 Сервер.
- СинтезМ-Клиент 8.6.
- СинтезМ-Сервер 8.6.

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

- Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
- CentOS Stream 9.

- EulerOS 2.0 SP10.
- SUSE Linux Enterprise Server 15.
- Ubuntu 22.04 LTS.
- Альт СП Рабочая Станция релиз 10.
- Альт СП Сервер релиз 10.
- РЕД ОС 8.0.

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 входящих и исходящих сообщений электронной почты;

· 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;

· получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);

· 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;

· исключения процессов из проверки памяти процессов в общих параметрах программы;

· оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles;

· исключения трафика из проверки программой;

· использовать формат JSON для запросов и вывода информации, а также для экспорта и импорта параметров программы и параметров задач;

· установки и работы на устройствах с операционными системами для архитектуры Arm;

· работать в режиме информирования пользователя в случае обнаружения угроз или при обнаружении попытки доступа к устройству;

· возможность управлять запуском приложений на защищаемых устройствах с помощью правил контроля в режимах списка запрещенных или разрешенных приложений;

· автоматический перезапуск приложения при обновлении;

· возможность задать ограничение на использование ресурсов процессора;

· возможность в автоматическом режиме выключить компоненты защиты и задачи проверки при запуске приложения после установки;

· уведомления пользователя о работе компонентов и задач в графическом пользовательском интерфейсе;

· возможность читать память процессов, не останавливая их (ядра Linux начиная с версии 3.4);

· возможность управлять доступом пользователей к веб-ресурсам;

· возможность управлять запуском приложений на защищаемых устройствах;

· функция мониторинга стабильности собственной работы приложения;

· защита от эксплойтов с возможностью настройки исключения объектов из проверки;

· возможность настроить список пользователей или групп пользователей контроля устройств, для которых добавленные устройства будут доверенными;

· возможность разрешать доступ к устройствам хранения данных только на чтение;

· возможность настраивать исключения для отдельных компонентов приложения при использовании прокси-сервера;

· возможность настраивать исключения из перехвата трафика;

· возможность временного исключения из проверки файлов журналов баз данных;

· возможность экспорта и импорта списков исключений в политиках и задачах, применяемых к приложению;

· возможность настраивать отмену запуска запланированных задач на устройстве, работающем от аккумулятора;

· возможность вывода списка функций приложения в командной строке, информацию об их статусах (используется или не используется) и технологиях Linux, с помощью которых реализованы эти функции приложения;

· возможность защиты от атак типа BadUSB;

· возможность отображать в командной строке и в графическом интерфейсе информацию о действующей на устройстве политике и профилях политики.

Требования к программным средствам антивирусной защиты мобильных устройств

Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:

o Android 5.0 и выше (включая Android 12L, исключая Go Edition);

o iOS 15 и выше или iPadOS 15 и выше;

В программном средстве антивирусной защиты смартфонов для ОС Android должны быть реализованы следующие функциональные возможности:

· постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;

· проверка файловой системы устройства по требованию и по расписанию;

· мгновенная проверка устанавливаемых приложений

· блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;

· наличие хранилища для изолирования зараженных объектов;

· обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;

· блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;

· поддержка белых списков разрешенных приложений;

· блокировка системных приложений, в рамках контроля запуска приложений;

· отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);

· заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;

· указать параметры подключения к wi-fi сетям;

· указать обязательные к установке приложения;

· блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);

· создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;

· поддержка технологий Samsung KNOX1 и KNOX2;

· указать разрешенные версии приложений при создании правил Контроля приложений для Androidустройств.

В программном средстве защиты смартфонов для ОС Apple iOS должны быть реализованы следующие функциональные возможности:

· удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;

· отправки команды блокирования и удаления данных;

· создавать групповые политики безопасности мобильных устройств;

· удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;

· получать отчеты и статистику о работе мобильных устройств пользователей;

· блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;

· централизованного управления с помощью единой консоли управления;

· наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.

· запретить изменение настроек Bluetooth для iOS MDMустройств

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 Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.

o Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSB) 64-разрядная.

o Windows Server 2019 Standard/Datacenter/Core 64-разрядная.

o Windows Server 2022 Standard/Datacenter/Core 64-разрядная.

o Windows Server 2025 Standard/Datacenter/Core 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 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 18.

o Oracle VM VirtualBox 7.x.

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

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

o Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная.

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

o Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная.

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

o MySQL 8.0 Community 32-разрядная/64-разрядная.

o MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.

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

o PostgreSQL 13.x 64-разрядная.

o PostgreSQL 14.x 64-разрядная.

o PostgreSQL 15.x 64-разрядная.

o Postgres Pro 13.x Windows/Linux 64-разрядная.

o Postgres Pro 14.x Windows/Linux 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 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;

· возможность управления развертыванием ОС Windows через консоль управления;

· наличие преднастроенных ролей пользователей средств централизованного управления;

· должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;

· возможность подключения по RDP или штатными средствами из консоли управления;

· наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing);

· пользователю должен выводиться запрос на разрешение дистанционного подключения;

· наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal);

· должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;

· возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС;

· возможность импортировать образ операционной системы из дистрибутивов (WIM)

· наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;

· автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры;

· поддержка функциональности управления шифрованием данных;

· возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF

· 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.

· автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей и серверах под управлением Microsoft Windows;

· возможность развернуть Сервер администрирования как систему высокой доступности;

· возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети.

· удаленная диагностика клиентских устройств на базе Windows и Linux (получение трассировок, журналов событий, дампов, остановка и запуск приложений);

· возможность отозвать права локального администратора учетных записей на управляемых устройствах с операционной системой Linux;

· возможность изменить пароль локальной учетной записи на управляемых устройствах с операционной системой Linux.

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 12 (Bookworm) 64-разрядная.

o Debian GNU/Linux 13 (Trixie) 64-разрядная.

o Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.

o Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.

- CentOS Stream 9 64-разрядная.
- CentOS Stream 10 64-разрядная.
- Red Hat Enterprise Linux Server 7.x 64-разрядная.
- Red Hat Enterprise Linux Server 8.x 64-разрядная.
- Red Hat Enterprise Linux Server 9.x 64-разрядная.
- Red Hat Enterprise Linux Server 10.x 64-разрядная.
- SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
- SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная.
- Astra Linux Special Edition RUSB.10015-03 (очередное обновление 7.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная.
- Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
- Альт СП Сервер 10 64-разрядная.
- Альт СП Рабочая станция 10 64-разрядная.
- Oracle Linux 7 64-разрядная.
- Oracle Linux 8 64-разрядная.
- Oracle Linux 9 64-разрядная.
- Platform V SberLinux OS Server (SLO) 8.10.1 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.5.1 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.6 64-разрядная.

- РЕД ОС 7.3 Сервер 64-разрядная.
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
- РЕД ОС 8 64-разрядная.
- РОСА "КОБАЛЬТ" 7.9 64-разрядная.
- М ОС (Moscow Electronic School) 12 Сервер 64-разрядная.
- Mostech Server 64-разрядная.
- МосОС 15.5 Arbat 64-разрядная.

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

- VMware vSphere 6.7.0.
- VMware vSphere 7.0.3.
- Microsoft Hyper-V Server 2019 64-разрядная.
- Microsoft Hyper-V Server 2022 64-разрядная.
- Citrix XenServer 7.x.
- Citrix XenServer 8.2.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.0.12.
- Kernel-based Virtual Machine (все поддерживаемые ОС Linux).

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

- MySQL 5.7 Community 32-разрядная/64-разрядная.
- MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
- MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
- MySQL Standard Edition 8.4 32-разрядная/64-разрядная.
- MySQL Enterprise Edition 8.4 32-разрядная/64-разрядная.

- MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.4 (сборка 10.4.20 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.5 (сборка 10.5.27 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.6 (сборка 10.6.20 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.11 (сборка 10.11.10 и выше) 32-разрядная/64-разрядная.
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- PostgreSQL 13.x 64-разрядная.
- PostgreSQL 14.x 64-разрядная.
- PostgreSQL 15.x 64-разрядная.
- PostgreSQL 15.x 64-разрядная (кластер Corosync/Pacemaker).
- PostgreSQL 16.x 64-разрядная.
- PostgreSQL 17 64-разрядная.
- PostgreSQL 18 64-разрядная.
- Postgres Pro 13.x (все редакции) 64-разрядная.
- Postgres Pro 14.x (все редакции) 64-разрядная.
- Postgres Pro 15.x (все редакции) 64-разрядная.
- Postgres Pro 15.x 64-разрядная (кластер Corosync/Pacemaker).
- Postgres Pro 16.x (все редакции) 64-разрядная.
- Postgres Pro 16.x Enterprise 64-разрядная (кластер Built-in High Availability).
- Postgres Pro 17 (все редакции) 64-разрядная.
- Postgres Pro 17 Enterprise 64-разрядная (кластер Built-in High Availability).
- Postgres Pro 18 (все редакции) 64-разрядная.
- Postgres Pro 18 Enterprise 64-разрядная (кластер Built-in High Availability).

- Platform V Pangolin 6.5.1 64-разрядная.
- Platform V Pangolin 6.5.1 64-разрядная (кластер Built-in High Availability).
- Jatoba 4 64-разрядная.
- Jatoba 5 64-разрядная.
- Tantor SE 1C 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;

· двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;

· создание резервной копии системы управления встроенными средствами системы управления;

· наличие системы контроля возникновения вирусных эпидемий;

· управления антивирусной защитой с использованием WEB консоли;

· 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;

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

· использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули;

· возможность передачи ключей шифрования между серверами централизованного управления;

· выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных;

· возможность экспорта и импорта выборок событий;

· возможность экспорта событий в SIEM-систему в форматах CEF или LEEF;

· возможность управления мобильными устройствами на Android и iOS;

· получение информации о программах, установленных на управляемые устройства;

· автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей и серверах под управлением Microsoft Windows;

· возможность поиска устройств по контроллерам доменов Microsoft Active Directory и Samba;

· возможность автоматизированного переноса данных с сервера администрирования под управлением ОС Windows на сервер администрирования под управлением ОС Linux;

· возможность удалённой диагностики управляемых устройств;

· поддержка кластерной технологии;

· возможность централизованного удаления несовместимого ПО с управляемых устройств;

· возможность централизованной перезагрузки управляемых устройств;

· возможность задать профили соединения для автономных пользователей с Linux-устройствами для подключения к одному и тому же или разным серверам централизованного управления в зависимости от местоположения устройства;

· поддержка контроллеров домена FreeIPA и ALD Pro;

· поддержка доменной аутентификации по Kerberos (технология единого входа, в том числе на основе сертификатов).

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

· 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 пользовател

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	Сарсеков Азиз Даниярович
Дата подписания	13.11.2026