Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасы Ішкі істер министрлігі Ақтөбе облысының Полиция департаменті" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасы Ішкі істер министрлігі Ақтөбе облысының Полиция департаменті" мемлекеттік мекемесі
Конкурстың №:	№ 17952736-1
Конкурстың атауы:	Ақтөбе облысы ПД қажеттілігі үшін антивирус лицензиясының мерзімін ұзарту қызметі.
Лоттың нөмірі:	№ 82838444-ОК2
Лоттың атауы	Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	582950.000.000000
Қызметтің атауы:	Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	43756681.03
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	43756681.03
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	Шарт күшіне енген сәттен бастап 16 күнтізбелік күн
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	36
Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Жалпы талаптар Антивирустық құралдар мыналарды қамтуы тиіс: Windows жұмыс станцияларына арналған антивирустық қорғаныс бағдарламалық құралдарын; Windows файлдық серверлеріне арналған құралдарды; Mac жұмыс станцияларына арналған құралдарды; Linux жұмыс станциялары мен серверлеріне арналған құралдарды; мобильді құрылғыларға (смартфондар мен планшеттерге) арналған құралдарды; орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарын; зиянды бағдарламалар мен шабуылдар сигнатураларының жаңартылып отыратын дерекқорларын; орыс тіліндегі пайдалану құжаттамасын. Барлық антивирустық құралдардың, оның ішінде басқару құралдарының, бағдарламалық интерфейсі орыс және ағылшын тілдерінде болуы тиіс. Барлық антивирустық құралдарда, оның ішінде басқару құралдарында, орыс және ағылшын тілдеріндегі контекстік анықтама жүйесі болуы тиіс. Windows жұмыс станцияларына арналған антивирустық қорғаныс бағдарламалық құралдарына қойылатын талаптар Антивирустық қорғаныс бағдарламалық құралдары келесі нұсқадағы жұмыс станцияларына арналған операциялық жүйелермен басқарылатын компьютерлерде жұмыс істеуі тиіс: o Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 және жоғары; Windows 8 Professional / Enterprise (32 / 64- биттік); Windows 8.1 Professional / Enterprise (32 / 64-биттік); Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise/Enterprise multi-session; Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise; Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise. Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы тиіс: • нысанның контекстік мәзірінен сұрау бойынша және нақты уақыт режимінде антивирустық сканерлеу; • кесте бойынша антивирустық сканерлеу; • қосылатын құрылғыларды антивирустық сканерлеу; • бұрын белгісіз зиянды бағдарламаларды анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдағыш; • белсенді жұқтыру әрекеттерін бейтараптандыру; • қолданбаның мінез-құлқын және оның жүйедегі әрекеттерін талдау арқылы оның зиянды белсенділігін анықтау және рұқсатсыз әрекеттерді табу; • желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау мақсатында ортақ қалталар мен файлдарға жүгінулерді талдау; • ортақ қолжетімді қалталарды сыртқы шифрлаудан қорғау функциясы үшін қорғау аймағын қалыптастыру; • бағдарламалық жасақтамадағы осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестер жадын қорғау; • емдеу кезінде зиянды бағдарламалық жасақтама әрекеттерін кері қайтару, оның ішінде зиянды бағдарламалармен шифрланған файлдарды қалпына келтіру; • процестер мен қолданбалар үшін артықшылықтарды шектеу (тізілімге жазу, файлдарға, қалталарға және басқа процестерге қолжетімділік, тапсырмалар жоспарлаушысына жүгіну, құрылғыларға қолжетімділік, нысандарға құқықтарды өзгерту және т.б.), сенім деңгейін анықтаумен динамикалық жаңартылатын, теңшелетін қолданбалар тізімдері;

	•қолданбаға іске қосылатын бағдарлама немесе файл бойынша үкім алу үшін нақты уақыт режимінде өндіруші ресурстарына жүгінуге мүмкіндік беретін жаңа қатерлерден бұлттық қорғаныс; • келесі форматтағы архивтердегі файлдарды антивирустық тексеру және емдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • келесі хаттамалар бойынша берілетін кіріс және шығыс трафикті тексерумен электрондық поштаны зиянды бағдарламалардан қорғау: IMAP, SMTP, POP3, MAPI, NNTP; • берілген түрдегі файлдарды қайта атау немесе жою мүмкіндігі бар пошта тіркемелерінің сүзгісі; • пайдаланушы компьютеріне HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP хаттамалары бойынша келетін желілік трафикті тексеру, оның ішінде эвристикалық талдау арқылы, сенімді ресурстарды теңшеу мүмкіндігімен және бұғаттау немесе статистика режимінде жұмыс істеумен; • жүктелетін веб-беттердегі баннерлер мен қалқымалы терезелерді бұғаттау; • фишингтік және қауіпсіз емес сайттарды анықтау және бұғаттау; • желілік пакеттік ережелер мен бағдарламалар үшін желілік ережелер жасауға мүмкіндік беретін, желі сегменттерін санаттауға болатын кірістірілген желіаралық экран; • кез келген түрдегі есептеу желілерінде қолданбалар мен порттар үшін желіаралық экран ережелерін пайдалану арқылы желілік шабуылдардан қорғау; • құрылғының MAC- мекенжайын жалғандауда ARP хаттамасының осалдықтарын пайдаланатын желілік қатерлерден қорғау; • бірнеше желілік қосылымды бір мезгілде орнатуды бұғаттау мүмкіндігімен желілік көпір түріндегі желілік қосылымдарды бақылау; • барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат ететін арнайы ережелер жасау; компонент қолданбаларды бағдарламаның орналасқан жолы, метадеректері, сертификаты немесе оның саусақ ізі, бақылау сомасы бойынша, сондай-ақ бағдарламалық жасақтама өндірушісі ұсынатын алдын ала берілген қолданба санаттары бойынша бақылауы тиіс; компонент қара немесе ақ тізім режимінде, сондай-ақ статистика жинау немесе бұғаттау режимінде жұмыс істеуі тиіс; • пайдаланушының құрылғы түрі және/немесе қолданылатын шина бойынша сыртқы енгізу/шығару құрылғыларымен жұмысын бақылау, олардың идентификаторы бойынша сенімді құрылғылар тізімін жасау мүмкіндігімен және Active Directory-дегі белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігімен; • құрылғыларды бақылау аясында MTP құрылғыларын басқару және барлық немесе пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін осы түрдегі құрылғыларға қолжетімділік ережелерін теңшеу; • ауыстырмалы дискілерде файлдарды жазу және/немесе жою туралы оқиғалар журналына жазба енгізу; • файлдық жүйесі бар құрылғыларға қолжетімділік ережелері үшін басымдық тағайындау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, өңдеу, өндіруші жасаған және динамикалық жаңартатын белгілі бір мазмұндағы, санаттағы ресурстарға, сондай-ақ

	ақпарат түріне (аудио, видео және т.б.) қолжетімділікке нақты тыйым салуды немесе рұқсат етуді қосу; бақылаудың уақыт аралықтарын енгізуге, сондай-ақ оны тек Active Directory-дегі белгілі бір пайдаланушыларға тағайындауға мүмкіндік беру; • BadUSB түріндегі шабуылдардан қорғау; • қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ құпия сөз арқылы қолданба параметрлеріне қолжетімділікті қорғау; • сенімді қашықтан әкімшілендіру бағдарламалары арқылы параметрлерді басқару; • антивирустық қорғаныс бағдарламалық құралының тек таңдалған компоненттерін орнату; • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару; • тапсырмаларды кесте бойынша және/немесе қолданба іске қосылғаннан кейін бірден іске қосу; • файлдық кеңістікті сканерлеу кезінде пайдаланушылардың жайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару; • соңғы тексеруден бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету; • антивирустық бағдарламаның тұтастығын тексеру; • файлдың бақылау сомасы, атау/каталог маскасы бойынша немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден алып тастауларды қосу; • ережелер мен алып тастаулар тізімдерін XML форматына импорттау және экспорттау; • антивируста жойылған жұқтырылған файлдарға арналған, оларды қалпына келтіру мүмкіндігі бар қорғалған қойманың болуы; • антивирустың жұмысы туралы есептерге арналған қорғалған қойманың болуы; • антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктердің ең аз жиынтығы бар графикалық интерфейстің жеңілдетілген нұсқасының болуы; • Windows Defender Security Center жүйесімен интеграция; • Antimalware Scan Interface (AMSI) қолдауының болуы; • Windows Subsystem for Linux (WSL) қолдауының болуы; • резервтік қоймадан нысандарды қалпына келтіруді құпия сөзбен қорғау; • интернетке қосылым лимитті болған жағдайда желілік трафикті шектеу; • TCP және UDP хаттамалары бойынша желіні мониторингілеу құралының болуы; • қайта жүктеуден кейін тексеру тапсырмасын тексеру тоқтатылған жерден жалғастыру; • тапсырманы орындау ұзақтығына шектеу орнату; • тексеру тапсырмаларын, тексеру әлдеқашан орындалып жатса, кезекке қою мүмкіндігі; • жүйені қайта жүктеусіз жаңарту; • Android Debug Bridge (ADB) қолданбасында пайдаланушылардың мобильді құрылғыларға қолжетімділігін теңшеу; • мобильді құрылғыға қолжетімділікке тыйым салынған жағдайда да, оны компьютерге USB арқылы қосу арқылы зарядтау; • пайдаланушылар үшін басып шығару құқықтарын теңшеу; • Wi-Fi желілеріне қосылымды бақылау үшін WPA3 хаттамасы қолдауының болуы; • Azure WVD жүйесімен үйлесімділіктің болуы; • iTunes қолданбасында пайдаланушылардың мобильді құрылғыларға қолжетімділігін теңшеу; • компьютерге орнатылған қолданбалардағы осалдықтарды анықтау және жабу үшін арнайы тапсырманы іске қосу, анықталған осалдықтар бойынша есеп беру мүмкіндігімен. • арнайы жүктеу агентін жасаумен және Single Sign On технологиясын қолдаумен

	толық дискілік шифрлау, UEFI жүйелерін қолдау; • жүктеу агентінде немесе ОЖ файлдарында ақаулар болған жағдайда шифрланған мазмұнды қалпына келтіру, UEFI жүйелерін қолдау; • толық дискілік шифрлау кезінде екі факторлы аутентификацияны қолдау; • шифрланатын мазмұнды икемді түрде көрсету мүмкіндігімен файлдарды шифрлау (орналасуы, кеңейтімі, файлды жасайтын қолданба бойынша); • таңдалған қолданбалар тарапынан шифрланған файлдарға қолжетімділікті шектеу тетіктерінің болуы, сондай-ақ ұйым шегінен тыс құпия сөз арқылы файлдарды дешифрлеуге мүмкіндік беретін технологияның болуы; • ұйым желісінен тыс файлдарды шифрлауға және дешифрлеуге мүмкіндік беретін жұмыс режимін белгілеу мүмкіндігімен ауыстырмалы тасығыштардағы деректерді шифрлау; • бағдарламалардың мінез-құлық үлгісін қалыптастыру және мінез-құлық үлгісінен ауытқыған жағдайда олардың әрекеттерін бұғаттау мүмкіндігі (аномалияларды бейімделмелі бақылау) • дискіні шифрлау кезінде аутентификация агентінің қызметтік есептік жазбасын жасау мүмкіндігі; • толық дискілік шифрлау кезінде SSO жұмысы үшін ADSelfService Plus сыртқы есептік деректер провайдерін қолдау; • енгізу құрылғыларынан басқа барлық Bluetooth құрылғыларына қолжетімділікті шектеу және ерекшеліктерді теңшеу мүмкіндігі; • операциялық жүйені қайта жүктеусіз қолданбаны жаңарту мүмкіндігі; • зиянды БЖ іздеу тапсырмасы үшін процессор ресурстарының тұтынылуын шектеу мүмкіндігі; • қолданба қызметтерін сырттан басқаруға тыйым салу мүмкіндігі; • тексеруден алдын ала орнатылған ерекшеліктер мен сенімді қолданбаларды таңдау мүмкіндігі; • жеке пайдаланушыға параметрлерді конфигурациялық файлға экспорттауға рұқсат беру мүмкіндігі; • құпия сөздер тарихын сақтауға (30 күнге дейін) және мәртебесін бақылауға (Белсенді, Мерзімі өткен, Кері қайтарылған) мүмкіндік беретін, қолданбаға қолжетімділікке арналған уақытша құпия сөздерді мониторингілеу және кері қайтарып алу мүмкіндігі; • саясат қолданылғаннан кейін бірден Веб-бақылау ережелерімен тыйым салынған веб-ресурстарға қосылымды үзу мүмкіндігі; • орнату дестесінде операциялық жүйелердің әртүрлі түрлері үшін компоненттердің әртүрлі жиынтығын теңшеу мүмкіндігі; • тексеруден алдын ала орнатылған ерекшеліктер мен сенімді қолданбаларды таңдау мүмкіндігі; • ескірген TLS 1.0 хаттамасы бойынша желілік қосылымдарды бұғаттау мүмкіндігі; • интернетке қолжетімділік үшін прокси-сервер арқылы қолданбаны аутентификациялауға арналған Kerberos хаттамасын қолдау; • қолданбаны тексеруден алып тастау үшін файл хешін көрсету мүмкіндігі. Windows серверлеріне арналған антивирустық қорғаныс бағдарламалық құралдарына қойылатын талаптар Антивирустық қорғаныс бағдарламалық құралдары келесі нұсқадағы файлдық серверлерге арналған операциялық жүйелермен басқарылатын компьютерлерде жұмыс істеуі тиіс: o Windows Small Business Server 2011 Essentials / Standard (64-биттік), Microsoft Small Business Server 2011 Standard (64-биттік) тек Microsoft Windows Server 2008 R2 үшін Service Pack 1 орнатылған жағдайда ғана қолдау көрсетіледі; Windows

	MultiPoint Server 2011 (64-биттік); Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 және жоғары; Windows Web Server 2008 R2 Service Pack 1 және жоғары; Windows Server 2012 Foundation / Essentials / Standard / Datacenter (Server Core режимін қоса алғанда); Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (Server Core режимін қоса алғанда); Windows Server 2016 Essentials / Standard / Datacenter (Server Core режимін қоса алғанда); Windows Server 2019 Essentials / Standard / Datacenter (Server Core режимін қоса алғанда); Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Server Core режимін қоса алғанда), Windows Server 2025 Standard / Datacenter. Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы тиіс: • нысанның контекстік мәзірінен сұрау бойынша және нақты уақыт режимінде антивирустық сканерлеу; • кесте бойынша антивирустық сканерлеу; • қосылатын құрылғыларды антивирустық сканерлеу; • бұрын белгісіз зиянды бағдарламаларды анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдағыш; • белсенді жұқтыру әрекеттерін бейтараптандыру; • қолданбаның мінез-құлқын және оның жүйедегі әрекеттерін талдау арқылы оның зиянды белсенділігін анықтау және рұқсатсыз әрекеттерді табу; • желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау мақсатында ортақ қалталар мен файлдарға жүгінулерді талдау; • бағдарламалық жасақтамадағы осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестер жадын қорғау; • емдеу кезінде зиянды бағдарламалық жасақтама әрекеттерін кері қайтару, оның ішінде зиянды бағдарламалармен шифрланған файлдарды қалпына келтіру; • қолданбаға іске қосылатын бағдарлама немесе файл бойынша үкім алу үшін нақты уақыт режимінде өндіруші ресурстарына жүгінуге мүмкіндік беретін жаңа қатерлерден бұлттық қорғаныс; • келесі форматтағы архивтердегі файлдарды антивирустық тексеру және емдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • желілік пакеттік ережелер мен бағдарламалар үшін желілік ережелер жасауға мүмкіндік беретін, желі сегменттерін санаттауға болатын кірістірілген желіаралық экран; • құрылғының MAC-мекенжайын жалғандауда ARP хаттамасының осалдықтарын пайдаланатын желілік қатерлерден қорғау; • қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалар, залымдар немесе біліктілігі жеткіліксіз пайдаланушылар тарапынан қорғанысты өшіруге жол бермеу үшін құпия сөз арқылы қолданба параметрлеріне қолжетімділікті қорғау; • антивирустық қорғаныс бағдарламалық құралының тек таңдалған компоненттерін орнату; • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару; • тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; • файлдық кеңістікті сканерлеу кезінде пайдаланушылардың жайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару; • соңғы

	тексеруден бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету; • антивирустық бағдарламаның тұтастығын тексеру; • файлдың бақылау сомасы, атау/каталог маскасы бойынша немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден алып тастауларды қосу; • антивируста жойылған жұқтырылған файлдарға арналған, оларды қалпына келтіру мүмкіндігі бар қорғалған қойманың болуы; • антивирустың жұмысы туралы есептерге арналған қорғалған қойманың болуы; • антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктердің ең аз жиынтығы бар графикалық интерфейстің жеңілдетілген нұсқасының болуы; • Windows Defender Security Center жүйесімен интеграция; • Antimalware Scan Interface (AMSI) қолдауының болуы; • Windows Subsystem for Linux (WSL) қолдауының болуы; • резервтік қоймадан нысандарды қалпына келтіруді құпия сөзбен қорғау. • ережелер мен алып тастаулар тізімдерін XML форматына импорттау және экспорттау; • интернетке қосылым лимитті болған жағдайда желілік трафикті шектеу; • барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат ететін арнайы ережелер жасау; компонент қолданбаларды бағдарламаның орналасқан жолы, метадеректері, сертификаты немесе оның саусақ ізі, бақылау сомасы бойынша, сондай-ақ бағдарламалық жасақтама өндірушісі ұсынатын алдын ала берілген қолданба санаттары бойынша бақылауы тиіс; компонент қара немесе ақ тізім режимінде, сондай-ақ статистика жинау немесе бұғаттау режимінде жұмыс істеуі тиіс; • компьютерге орнатылған қолданбалардағы осалдықтарды анықтау және жабу үшін арнайы тапсырманы іске қосу, анықталған осалдықтар бойынша есеп беру мүмкіндігімен; • Windows серверлеріне арналған операциялық жүйемен басқарылатын компьютерлер үшін Веб-қатерлерден қорғау, Пошта қатерлерінен қорғау, Веб-бақылау және Құрылғыларды бақылау компоненттерін қолдау. • қайта жүктеуден кейін тексеру тапсырмасын тексеру тоқтатылған жерден жалғастыру; • тапсырманы орындау ұзақтығына шектеу орнату мүмкіндігі; • тексеру тапсырмаларын, тексеру әлдеқашан орындалып жатса, кезекке қою мүмкіндігі; • жүйені қайта жүктеусіз жаңарту; • портативті құрылғылар (MTP) үшін қолжетімділік құқықтарын (оқу / жазу) теңшеу, құрылғыларға қолжетімділігі бар пайдаланушыларды немесе пайдаланушылар тобын таңдау, сондай-ақ құрылғыларға қолжетімділік кестесін белгілеу; • мобильді құрылғыға қолжетімділікке тыйым салынған жағдайда да, оны компьютерге USB арқылы қосу арқылы зарядтау; • пайдаланушылар үшін басып шығару құқықтарын теңшеу; • Wi-Fi желілеріне қосылымды бақылау үшін WPA3 хаттамасы қолдауының болуы; • Azure WVD жүйесімен үйлесімділіктің болуы; • операциялық жүйені қайта жүктеусіз қолданбаны жаңарту мүмкіндігі; • зиянды БЖ іздеу тапсырмасы үшін процессор ресурстарының тұтынылуын шектеу мүмкіндігі. • қолданба қызметтерін сырттан басқаруға тыйым салу мүмкіндігі. • SQL-серверлерде, Microsoft

	Exchange серверлерінде және System Center Configuration Manager-де қолданбаның жұмысы үшін сенімді аймақты жылдам теңшеуге арналған, тексеруден алдын ала орнатылған ерекшеліктер мен сенімді қолданбаларды пайдалану мүмкіндігі; • интернетке қолжетімділік үшін прокси-сервер арқылы қолданбаны аутентификациялауға арналған Kerberos хаттамасын қолдау; • қолданбаны тексеруден алып тастау үшін файл хешін көрсету мүмкіндігі. Mac жұмыс станцияларына арналған антивирустық қорғаныс бағдарламалық құралдарына қойылатын талаптар Mac жұмыс станцияларына арналған антивирустық қорғаныс бағдарламалық құралдары келесі нұсқадағы операциялық жүйелермен басқарылатын компьютерлерде жұмыс істеуі тиіс: o macOS 12 - 15; Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы тиіс: • резиденттік антивирустық мониторинг; • қолданбаға іске қосылатын бағдарлама немесе файл бойынша үкім алу үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қатерлерден бұлттық қорғаныс; • антивирустық дерекқорларды кесте бойынша автоматты түрде жаңарту; • қалпына келтіру мүмкіндігі үшін жұқтырылған файлдарды жоюдың алдында резервтік көшірмелеу; • бұрын белгісіз зиянды бағдарламаларды анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдағыш; • кез келген түрдегі, оның ішінде сымсыз, есептеу желілерінде жұмыс істеу кезінде ең танымал қолданбалар үшін кіруді анықтау және болдырмау жүйесін (IDS/IPS) және желілік белсенділік ережелерін пайдалану арқылы желілік шабуылдардан қорғау; • антивирустық қорғаныс құралдары өндірушісінің репутациялық бұлттық қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды бұғаттау; • Safari, Google Chrome және Firefox браузерлері арқылы берілетін желілік трафикті (HTTP және HTTPS трафик) тексеру; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, өңдеу, өндіруші жасаған және динамикалық жаңартатын белгілі бір ресурстарға немесе ресурс санаттарына қолжетімділікке нақты тыйым салуды немесе рұқсат етуді қосу • соңғы тексеруден бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету; • файлдық операцияларды ұстап алу деңгейінде көрсетілген аймақтарды тексеру кезінде ерекшеліктерді белгілеу; • дискіге толық қолжетімділік құқықтарының пайда болуын автоматты түрде қадағалау және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнату; • зиянды БЖ іздеу тапсырмаларын орындау кезінде қолданбаның процессорды жүктеуін шектеу; • операциялық жүйе ресурстарына жүктемені азайту үшін бұлттық режимді қосу және зиянды БЖ дерекқорларының жеңілдетілген нұсқасын пайдалану; • сұрау бойынша тексеру тапсырмаларын орындау кезінде тек оқуға қолжетімді жүйелік томды сканерлеуден өткізіп жіберу; • қауіпті мінез-құлық үлгілерін (BSS) пайдалану арқылы операциялық жүйедегі қолданбалар белсенділігін талдау; • JAMF арқылы .pkg файлынан орнату; • сыртқы дискілерді қосқан кезде оларды автоматты түрде сканерлеу; • клиенттік сертификаттарды

	қолдау; • кіріс және шығыс электрондық пошта хабарламаларының тіркемелерін зиянды БЖ мен басқа қатерлердің бар-жоғына тексеру; • пайдаланушылардың компьютерге орнатылған немесе қосылған құрылғыларға қолжетімділігін басқару; • интернетте немесе жергілікті желіде жұмыс істеу кезінде компьютерге рұқсатсыз қосылымдарды бұғаттау және қолданбалардың желілік белсенділігін бақылау; • зиянды бағдарламалық жасақтаманың ОЖ-дағы файлдық, жүйелік немесе желілік белсенділігімен байланысты әрекеттерін кері қайтару; • эксплойттардан қорғау. • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару. Linux жұмыс станциялары мен серверлеріне арналған антивирустық қорғаныс бағдарламалық құралдарына қойылатын талаптар Linux жұмыс станцияларына арналған антивирустық қорғаныс бағдарламалық құралдары келесі нұсқадағы 32-биттік операциялық жүйелермен басқарылатын компьютерлерде жұмыс істеуі тиіс: o Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12 Linux жұмыс станцияларына арналған антивирустық қорғаныс бағдарламалық құралдары келесі нұсқадағы 64-биттік операциялық жүйелермен басқарылатын компьютерлерде жұмыс істеуі тиіс: o 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 (кезекті жаңарту 1.5); Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.6); Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.7); Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.8); Astra Linux Special Edition РУСБ.10015-03 (кезекті жаңарту 7.6); Astra Linux Special Edition РУСБ.10015-16 (1-нұсқа) (кезекті жаңарту 1.6); Astra Linux Special Edition РУСБ.10015-17 (кезекті жаңарту 1.7.3); Astra Linux Special Edition РУСБ.10015-37 (кезекті жаңарту 7.7); CentOS 7.2 - 7.9.; CentOS Stream 8-10; 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 - 7.9; Oracle Linux 8.5 - 8.9; Oracle Linux 9.4 - 9.6; Red Hat® Enterprise Linux® 7.2 - 7.9.; Red Hat Enterprise Linux 8.5 - 8.9.; Red Hat Enterprise Linux 9.4 - 9.6.; Red Hat Enterprise Linux 10.0, 10.1.; Rocky Linux 8.6 - 8.9.; Rocky Linux 9.4 - 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 - 15.7.; Ubuntu® 22.04 LTS.; Ubuntu 24.04 LTS.; Альт Образование 10, 11; Альт Рабочая Станция 11; Альт Сервер 11; Альт СП Сервер релиз 10; Альт СП Рабочая Станция релиз 10; Атлант, сборка Alcyone, нұсқа 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 Барлық пайдаланушылар үшін (телеметриясыз және ДИТ қолдауынсыз) release 2021.1.; ОС МЭШ 12 Мәскеу мектептеріне арналған, интерактивті тақталар үшін (телеметриямен және

	ДИТ қолдауымен) release 2021.1.; ОС МЭШ 12 Мәскеу мектептеріне арналған, компьютерлер мен ноутбуктер үшін (телеметриямен және ДИТ қолдауымен) 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. ARM архитектурасына арналған қолдау көрсетілетін 64-биттік операциялық жүйелер: о Astra Linux Special Edition РУСБ.10152-02 (кезекті жаңарту 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. Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы тиіс: • резиденттік антивирустық мониторинг; • қолданбаға іске қосылатын бағдарлама немесе файл бойынша үкім алу үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қатерлерден бұлттық қорғаныс; • SMB / NFS арқылы қолжетімді ресурстарды тексеру; • ядро жадын тексеру мүмкіндігі; • бұрын белгісіз зиянды бағдарламаларды тиімдірек анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдағыш; • пайдаланушының немесе әкімшінің командасы бойынша және кесте бойынша антивирустық сканерлеу; • келесі архивтердегі файлдарды антивирустық тексеру: zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.; • кіріс және шығыс электрондық пошта хабарламаларын тексеру; • файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытының лимиті, тексерілетін файл өлшемінің лимиті, тексерілген және тексеруден кейін өзгермеген файлдар туралы ақпаратты кештеу тетігі); • SMB / NFS хаттамалары бойынша желілік қолжетімділігі бар жергілікті каталогтардағы файлдарды қашықтан зиянды шифрлаудан қорғау; • тексеру кезінде файлдарды бұғаттау опциясын қосу; • күдікті және зақымдалған нысандарды карантинге орналастыру; • SAMBA деңгейінде файлдық операцияларды ұстап алу және тексеру; • операциялық жүйенің желіаралық экранын басқару, ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен; • тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; • есептерді HTML және CSV форматтарында экспорттау және сақтау; • файлдық кеңістікті сканерлеу кезінде пайдаланушылардың жайлы жұмысын қамтамасыз ету үшін ДК ресурстарын пайдалануды икемді басқару; • ақпараттық құндылығы бар жұқтырылған нысанды сұрау бойынша қалпына келтіру мүмкіндігі үшін оны емдеу мен жоюдың алдында резервтік қоймада көшірмесін сақтау; • root құқықтарынсыз пайдаланушының графикалық интерфейсі арқылы басқару; • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі немесе веб-консоль арқылы орталықтандырылған басқару; • пайдаланушылардың компьютерге орнатылған немесе қосылған құрылғыларға құрылғы түрі мен қосылым шинасы бойынша қолжетімділігін басқару; • ауыстырмалы дискілерді тексеру; • кіріс желілік

	трафиктегі желілік шабуылдарға тән белсенділікті қадағалау; • пайдаланушы компьютеріне HTTP/HTTPS және FTP хаттамалары бойынша келетін трафикті тексеру, сондай-ақ веб-мекенжайлардың зиянды немесе фишингтік екенін анықтау мүмкіндігі • пайдаланушы компьютеріндегі бағдарламалар әрекеттері туралы деректер алу; • компьютерлерде сақталатын бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу (Түгендеу тапсырмасы); • бағдарлама іске қосылған кезде трассировка файлдарын жасау; • компьютерлерге орнатылған бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу; • автоіске қосу нысандарын, жүктеу секторларын, процестер жады мен ядро жадын тексеру; • емдеу немесе жоюдың алдында файлдардың резервтік көшірмелерін сақтау және файлдарды резервтік көшірмелерден қалпына келтіру; • бағдарламаның жалпы параметрлерінде процестер жадын тексеруден процестерді алып тастау; • SkipPlainTextFiles параметрі арқылы бағдарламалар журналдарын тексеруді оңтайландыру; • трафикті бағдарламамен тексеруден алып тастау; • сұраулар мен ақпаратты шығару үшін, сондай-ақ бағдарлама параметрлері мен тапсырма параметрлерін экспорттау және импорттау үшін JSON форматын пайдалану; • Arm архитектурасына арналған операциялық жүйелері бар құрылғыларда орнату және жұмыс істеу; • қатерлер анықталған немесе құрылғыға қолжетімділік әрекеті байқалған жағдайда пайдаланушыны хабардар ету режимінде жұмыс істеу; • тыйым салынған немесе рұқсат етілген қолданбалар тізімі режимдерінде бақылау ережелері арқылы қорғалатын құрылғыларда қолданбалардың іске қосылуын басқару мүмкіндігі; • жаңарту кезінде қолданбаны автоматты түрде қайта іске қосу; • процессор ресурстарын пайдалануға шектеу белгілеу мүмкіндігі; • орнатудан кейін қолданба іске қосылған кезде қорғаныс компоненттері мен тексеру тапсырмаларын автоматты режимде өшіру мүмкіндігі; • графикалық пайдаланушы интерфейсінде компоненттер мен тапсырмалардың жұмысы туралы пайдаланушыны хабардар ету; • процестерді тоқтатпай олардың жадын оқу мүмкіндігі (3.4 нұсқасынан бастап Linux ядролары); • пайдаланушылардың веб-ресурстарға қолжетімділігін басқару мүмкіндігі; • қорғалатын құрылғыларда қолданбалардың іске қосылуын басқару мүмкіндігі; • қолданбаның өз жұмысының тұрақтылығын мониторингілеу функциясы; • нысандарды тексеруден алып тастауды теңшеу мүмкіндігі бар эксплойттардан қорғау; • қосылған құрылғылар сенімді болатын, құрылғыларды бақылауға арналған пайдаланушылар немесе пайдаланушылар топтарының тізімін теңшеу мүмкіндігі; • деректерді сақтау құрылғыларына тек оқу үшін қолжетімділік беру мүмкіндігі; • прокси- серверді пайдалану кезінде қолданбаның жекелеген компоненттері үшін ерекшеліктерді теңшеу мүмкіндігі; • трафикті ұстап алудан ерекшеліктерді теңшеу мүмкіндігі; • дерекқор журнал файлдарын тексеруден уақытша алып тастау мүмкіндігі; • қолданбаға қолданылатын саясаттар мен тапсырмалардағы алып тастаулар тізімдерін экспорттау және импорттау мүмкіндігі; • аккумулятордан жұмыс істейтін құрылғыда жоспарланған тапсырмалардың іске қосылуын

	болдырмауды теңшеу мүмкіндігі; • қолданба функцияларының тізімін командалық жолда шығару, олардың мәртебелері (пайдаланылады немесе пайдаланылмайды) және осы қолданба функциялары іске асырылған Linux технологиялары туралы ақпарат беру мүмкіндігі; • BadUSB түріндегі шабуылдардан қорғау мүмкіндігі; • командалық жолда және графикалық интерфейсте құрылғыда қолданылып жатқан саясат пен саясат профильдері туралы ақпаратты көрсету мүмкіндігі. Мобильді құрылғыларға арналған антивирустық қорғаныс бағдарламалық құралдарына қойылатын талаптар Смартфондарды антивирустық қорғауға арналған бағдарламалық құралдар келесі мобильді ОЖ басқаруымен жұмыс істеуі тиіс: o Android 5.0 және жоғары (Android 12L қоса алғанда, Go Edition-нан басқа); o iOS 15 және жоғары немесе iPadOS 15 және жоғары; Android ОЖ үшін смартфондарды антивирустық қорғау бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы тиіс: • антивирустық қорғаныс құралдары өндірушісінің бұлттық репутациялық қызметін пайдаланатын қосымша тексеру деңгейі бар, смартфонның файлдық жүйесін тұрақты антивирустық қорғау; • құрылғының файлдық жүйесін сұрау бойынша және кесте бойынша тексеру; • орнатылатын қолданбаларды лезде тексеру • антивирустық қорғаныс құралдары өндірушісінің репутациялық бұлттық қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды бұғаттау; • жұқтырылған нысандарды оқшаулауға арналған қойманың болуы; • зиянды бағдарламаларды іздеу және қауіпті нысандарды жою кезінде пайдаланылатын антивирустық дерекқорларды кесте бойынша жаңарту; • көрсетілген қолданбалардың іске қосылуын бұғаттау, оның ішінде алдын ала берілген қолданба санаттары арқылы; • рұқсат етілген қолданбалардың ақ тізімдерін қолдау; • қолданбалардың іске қосылуын бақылау аясында жүйелік қолданбаларды бұғаттау; • Firebase Cloud Messaging (FCM) қызметі арқылы командалар мен push хабарландыруларын жіберу; • wi-fi және bluetooth модульдерін, сондай- ақ мобильді құрылғы камерасын пайдалануды бұғаттау; • wi-fi желілеріне қосылу параметрлерін көрсету; • міндетті түрде орнатылуға тиіс қолданбаларды көрсету; • мобильді құрылғыны бұғаттау, деректерді жою, жұмыс қызметіне байланысты деректерді жою, құрылғының орналасу координаттарын алу, зауыттық параметрлерге қашықтан қайтару (factory reset); • сәйкессіздіктер анықталған жағдайда құрылғыны автоматты түрде бұғаттау, деректерді жою, корпоративтік қолданбалардың іске қосылуына тыйым салу мүмкіндігімен, мобильді құрылғыны корпоративтік саясаттарға сәйкестігіне тексеру негізінде жүзеге асырылатын ережелер тізімін жасау; • Samsung KNOX1 және KNOX2 технологияларын қолдау; • Android құрылғылары үшін Қолданбаларды бақылау ережелерін жасау кезінде қолданбалардың рұқсат етілген нұсқаларын көрсету. Apple iOS ОЖ үшін смартфондарды қорғау бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы тиіс: • топтық саясаттар арқылы iOS MDM құрылғыларының параметрлерін қашықтан теңшеу; • бұғаттау және деректерді жою командаларын жіберу; • мобильді құрылғылардың

	қауіпсіздік топтық саясаттарын жасау; • Exchange ActiveSync\ iOS MDM хаттамасы бойынша қосылған құрылғылардың конфигурациялық параметрлерін қашықтан теңшеу; • пайдаланушылардың мобильді құрылғыларының жұмысы туралы есептер мен статистика алу; • supervised mode пайдаланылған кезде антивирустық қорғаныс құралдары өндірушісінің репутациялық бұлттық қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды бұғаттау; • бірыңғай басқару консолі арқылы орталықтандырылған басқару; • басқарылатын құрылғыда iTunes, Safari немесе Game Center сияқты құрылғының меншікті қолданбаларын пайдалануға болатынын бақылауға мүмкіндік беретін компоненттің болуы. • iOS MDM құрылғылары үшін Bluetooth параметрлерін өзгертуге тыйым салу Windows ОЖ негізіндегі орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қойылатын талаптар Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқадағы операциялық жүйелермен басқарылатын компьютерлерде жұмыс істеуі тиіс: o Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64- биттік; Windows Server 2016 Standard/Datacenter/Essentials/Server Core (орнату нұсқалары) (LTSB) 64-биттік; Windows Server 2019 Standard/Datacenter/Core 64-биттік; Windows Server 2022 Standard/Datacenter/Core 64-биттік; Windows Server 2025 Standard/Datacenter/Core 64-биттік; Windows Storage Server 2019 64-биттік. Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі виртуалды платформаларда орнатылуды қолдауы тиіс: o VMware vSphere 6.7, 7.0; Microsoft Hyper-V Server 2019, 2022 (64-биттік); Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x.; Parallels Desktop 18.; Oracle VM VirtualBox 7.x. Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқадағы ДҚБЖ-мен жұмыс істеуі тиіс: o Microsoft SQL Server 2016 (барлық басылымдары) 64-биттік; Microsoft SQL Server 2017 (барлық басылымдары) Windows/Linux үшін 64-биттік; Microsoft SQL Server 2019 (барлық басылымдары) Windows/Linux үшін 64-биттік (қосымша әрекеттер қажет); Microsoft SQL Server 2022 (барлық басылымдары) Windows/Linux үшін 64-биттік; MySQL 5.7 Community 32-биттік/64-биттік; MySQL 8.0 Community 32-биттік/64-биттік; MariaDB 10.5 (10.5.17 құрастыруы және жоғары) 32-биттік/64-биттік; MariaDB Galera Cluster 10.3 32-биттік/64-биттік, InnoDB қойма ішкі жүйесімен; PostgreSQL 13.x 64-биттік; PostgreSQL 14.x 64-биттік; PostgreSQL 15.x 64-биттік; Postgres Pro 13.x Windows/Linux 64-биттік; Postgres Pro 14.x Windows/Linux 64-биттік. Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы тиіс: • қорғалатын түйіндер санына байланысты орталықтандырылған басқару, мониторинг және жаңарту құралының орнату архитектурасын таңдау; • ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректер алу мақсатында Active Directory-ден ақпарат оқу; • анықталған компьютерлерді ip-мекенжайы, ОЖ түрі, OU AD ішіндегі орналасуы бойынша

	тасымалдау ережелерін теңшеу; • желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтарына автоматты түрде бөлу; ip-мекенжайы, ОЖ түрі, OU AD ішіндегі орналасуы бойынша тасымалдау ережелерін теңшеу мүмкіндігі; • антивирустық қорғаныс бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою; • орталықтандырылған теңшеу, әкімшілендіру; • қорғаныс құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау; • басқару орталығы құралдары арқылы үйлесімсіз қолданбаларды орталықтандырылған жою (қолмен және автоматты); • саясаттар мен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға кері қайтару мүмкіндігі; • антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін – RPC, GPO, басқару жүйесі құралдары арқылы, жергілікті орнату үшін – автономды орнату дестесін жасау мүмкіндігі; • қауіпсіздік саясаттарында пайдаланушы жүйеге кірген есептік жазбаға, ағымдағы IPv4-мекенжайына, сондай-ақ компьютердің қай OU-де немесе қай қауіпсіздік тобында орналасқанына байланысты антивирустық шешім параметрлерін қайта анықтайтын арнайы триггерлерді көрсету; • қайта бөлу жүзеге асырылатын триггерлер иерархиясы; • жүктелген жаңартуларды клиенттік машиналарға таратудың алдында орталықтандырылған басқару БЖ құралдарымен тестілеу; • жаңартуларды пайдаланушылардың жұмыс орындарына алынғаннан кейін бірден жеткізу; • желідегі виртуалды машиналарды анықтау және егер бұл машиналар бір физикалық серверде орналаса, олардың арасында іске қосылатын тапсырмалардың жүктеме теңгерімін бөлу; • әр деңгейде әкімшілер мен операторлардың құқықтарын, сондай-ақ берілетін есептілік нысандарын теңшеу мүмкіндігі бар көпдеңгейлі басқару жүйесін құру; • кез келген деңгейдегі әкімшілендіру серверлерінің иерархиясын құру және жоғарғы деңгейден бүкіл иерархияны орталықтандырылған басқару мүмкіндігі; • басқару серверлері үшін мультиарендалықты (multi-tenancy) қолдау; • бағдарламалық құралдар мен антивирустық дерекқорларды әртүрлі көздерден, байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да жаңарту; • басқару сервері арқылы антивирустық БЖ өндірушісінің бұлттық серверлеріне қолжетімділік; • клиенттік компьютерлерге лицензияны автоматты түрде тарату; • пайдаланушылар компьютерлеріндегі орнатылған БЖ мен жабдықты түгендеу; • орнатылған антивирустық қорғаныс қолданбаларының жұмысындағы оқиғалар туралы хабарландыру тетігінің болуы және олар туралы пошта хабарландыруларын жіберуді теңшеу; • iOS MDM сервері арқылы мобильді құрылғыларды басқару функциясы; • берілген оқиғалар туралы SMS-хабарландыруларын жіберу; • басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; • басқару жүйесіне желілік жүктемені азайту үшін ұйымның кез келген компьютерін жаңартуларды ретрансляциялау орталығы ретінде көрсету; • басқару жүйесіне желілік жүктемені азайту үшін ұйымның кез келген компьютерін, таңдалған клиенттік компьютерлер тобының антивирустық агенттер оқиғаларын орталықтандырылған басқару

	серверіне жіберу орталығы ретінде көрсету; • антивирустық қорғаныс оқиғалары, түгендеу деректері, орнатылған бағдарламаларды лицензиялау деректері бойынша графикалық есептер құру; • жүйенің жұмысы туралы алдын ала теңшелген стандартты есептердің болуы; • есептерді PDF және XML форматындағы файлдарға экспорттау; • антивирустық бағдарламалық жасақтама орнатылған желінің барлық ресурстары бойынша резервтік қоймалар мен карантин нысандарын орталықтандырылған басқару; • басқару серверінде аутентификациялауға арналған ішкі есептік жазбаларды жасау; • басқару жүйесінің кірістірілген құралдарымен басқару жүйесінің резервтік көшірмесін жасау; • Windows Failover Clustering қолдауы; • Windows Certificate Authority қызметімен интеграцияны қолдау; • пайдаланушыларға арналған өзіне-өзі қызмет көрсету порталының болуы; • өзіне-өзі қызмет көрсету порталы пайдаланушыларға мобильді құрылғыға басқару агентін орнату, мобильді құрылғыларды қарау, бұғаттау командаларын жіберу, құрылғыны іздеу және пайдаланушының мобильді құрылғысындағы деректерді жою мақсатында қосылу мүмкіндігін қамтамасыз етуі тиіс; • вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы; • Microsoft Azure және Google Cloud бұлттық инфрақұрылымында орнату; • OpenAPI арқылы интеграция; • WEB консолін пайдаланып антивирустық қорғанысты басқару; • басқару консолі арқылы Windows ОЖ таратуды басқару мүмкіндігі; • орталықтандырылған басқару құралдарының алдын ала теңшелген пайдаланушы рөлдерінің болуы; • пайдаланушы есептік жазбаларына тіркеу үшін нақты көрсетілген өкілеттіктер жиынтығы бар мамандандырылған рөлдер жасау мүмкіндігі іске асырылуы тиіс; • басқару консолінен RDP арқылы немесе штаттық құралдармен қосылу мүмкіндігі; • Windows жұмыс үстеліне бірлескен қосылу мүмкіндігінің болуы (Windows Desktop Sharing); • пайдаланушыға қашықтан қосылуға рұқсат беру туралы сұрау көрсетілуі тиіс; • ОЖ бейнелерімен жұмыс істеу құралдарының болуы: физикалық немесе виртуалды машина негізінде мақсатты ОЖ бейнесін жасау, бейнені әкімші таңдаған компьютерлерге, оның ішінде "таза темірге" (bare metal) орнату; • бұрын жасалған бейнеге драйверлер жинақтарын қосу мүмкіндігі қамтамасыз етілуі тиіс; • ОЖ орнатылғаннан кейін автоматты режимде скрипттер іске қосу немесе қосымша БЖ орнату мүмкіндігі; • операциялық жүйе бейнесін дистрибутивтерден (WIM) импорттау мүмкіндігі • компьютерге орнатылған үшінші тарап БЖ лицензияларын бақылау жүйесінің болуы, лицензияны пайдалану ережесі бұзылған немесе лицензия мерзімі асып кеткен жағдайда әкімшіге хабарландыру мүмкіндігімен; • үшінші тарап қолданбалары үшін орнату дестелерін автоматты түрде жасау (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қолданба дестелерін компьютерлерге автоматты орталықтандырылған орнату; • деректерді шифрлауды басқару функционалдығын қолдау; • SIEM жүйелерімен интеграциялау және оқиғаларды syslog немесе CEF\LEEF форматында беру мүмкіндігі • Әкімшілендіру консоліне рұқсатсыз қолжетімділік қаупін азайту үшін екі кезеңдік тексеру; • пайдаланушы

	есептік жазбасының параметрлері өзгертілгеннен кейін қосымша аутентификацияны пайдалану. • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылар кездесетін желілерді сұрау мүмкіндігі. • Microsoft Windows басқаруындағы пайдаланушылар компьютерлері мен серверлеріндегі орнатылған қолданбалар мен операциялық жүйедегі осалдықтарды автоматтандырылған іздеу және жабу; • Әкімшілендіру серверін жоғары қолжетімділік жүйесі ретінде орналастыру мүмкіндігі; • оқшауланған желіде үшінші тарап өндірушілерінің (Microsoft бағдарламаларынан басқа) бағдарламаларының жаңартуларын орнату және осалдықтарын жабу мүмкіндігі. • Windows және Linux негізіндегі клиенттік құрылғыларды қашықтан диагностикалау (трассировкаларды, оқиғалар журналдарын, дамптарды алу, қолданбаларды тоқтату және іске қосу); • Linux операциялық жүйесі бар басқарылатын құрылғылардағы есептік жазбалардың жергілікті әкімші құқықтарын кері қайтарып алу мүмкіндігі; • Linux операциялық жүйесі бар басқарылатын құрылғылардағы жергілікті есептік жазбаның құпия сөзін өзгерту мүмкіндігі. Linux ОЖ негізіндегі орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қойылатын талаптар Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқадағы операциялық жүйелермен басқарылатын компьютерлерде жұмыс істеуі тиіс: o Debian GNU/Linux 12 (Bookworm) 64-биттік; Debian GNU/Linux 13 (Trixie) 64- биттік; Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-биттік; Ubuntu Server 24.04 LTS (Noble Numbat) 64-биттік; CentOS Stream 9 64-биттік; CentOS Stream 10 64-биттік; Red Hat Enterprise Linux Server 7.x 64- биттік; Red Hat Enterprise Linux Server 8.x 64-биттік; Red Hat Enterprise Linux Server 9.x 64-биттік; Red Hat Enterprise Linux Server 10.x 64- биттік; SUSE Linux Enterprise Server 12 (барлық жаңарту дестелері) 64- биттік; SUSE Linux Enterprise Server 15 (барлық жаңарту дестелері) 64- биттік; Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.6) 64-биттік; Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.7) 64-биттік; Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.8) 64-биттік; Astra Linux Special Edition РУСБ.10015-16 (1- нұсқа) (кезекті жаңарту 1.6) 64-биттік; Astra Linux Special Edition РУСБ.10015-17 (кезекті жаңарту 1.7.3) 64-биттік; Astra Linux Special Edition RUSB.10015-03 (кезекті жаңарту 7.6) 64-биттік; Astra Linux Special Edition РУСБ.10015-37 (кезекті жаңарту 7.7) 64-биттік; Astra Linux Common Edition (кезекті жаңарту 2.12) 64-биттік; Альт СП Сервер 10 64-биттік; Альт СП Рабочая станция 10 64-биттік; Oracle Linux 7 64- биттік; Oracle Linux 8 64-биттік; Oracle Linux 9 64-биттік; Platform V SberLinux OS Server (SLO) 8.10.1 64-биттік; Platform V SberLinux OS Server (SLO) 9.5.1 64-биттік; Platform V SberLinux OS Server (SLO) 9.6 64-биттік; РЕД ОС 7.3 Сервер 64-биттік; РЕД ОС 7.3 Сертифицированная редакция 64-биттік; РЕД ОС 8 64-биттік; РОСА "КОБАЛЬТ" 7.9 64-биттік; М ОС (Moscow Electronic School) 12 Сервер

	64-биттік; Mostech Server 64-биттік; МосОС 15.5 Arbat 64-биттік. Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі виртуалды платформаларда орнатылуды қолдауы тиіс: о VMware vSphere 6.7.0., 7.0.3; Microsoft Hyper-V Server 2019, 2022 (64-биттік); Citrix XenServer 7.x.; Citrix XenServer 8.2; Parallels Desktop 18; Oracle VM VirtualBox 7.0.12; Kernel-based Virtual Machine (барлық қолдау көрсетілетін Linux ОЖ). Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқадағы ДҚБЖ-мен жұмыс істеуі тиіс: о MySQL 5.7 Community 32-биттік/64-биттік; MySQL Standard Edition 8.0 (релиз 8.0.20 және жоғары) 32-биттік/64-биттік; MySQL Enterprise Edition 8.0 (релиз 8.0.20 және жоғары) 32-биттік/64-биттік; MySQL Standard Edition 8.4 32-биттік/64-биттік; MySQL Enterprise Edition 8.4 32-биттік/64-биттік; MariaDB 10.1 (10.1.30 құрастыруы және жоғары) 32-биттік/64-биттік; MariaDB 10.3 (10.3.22 құрастыруы және жоғары) 32-биттік/64-биттік; MariaDB 10.4 (10.4.20 құрастыруы және жоғары) 32-биттік/64-биттік; MariaDB 10.5 (10.5.27 құрастыруы және жоғары) 32-биттік/64-биттік; MariaDB 10.6 (10.6.20 құрастыруы және жоғары) 32-биттік/64-биттік; MariaDB 10.11 (10.11.10 құрастыруы және жоғары) 32-биттік/64-биттік; MariaDB Galera Cluster 10.3 32-биттік/64-биттік, InnoDB қойма ішкі жүйесімен; PostgreSQL 13.x 64-биттік; PostgreSQL 14.x 64-биттік; PostgreSQL 15.x 64-биттік; PostgreSQL 15.x 64-биттік (Corosync/Pacemaker кластері); PostgreSQL 16.x 64-биттік; PostgreSQL 17 64-биттік; PostgreSQL 18 64-биттік; Postgres Pro 13.x (барлық басылымдары) 64-биттік; Postgres Pro 14.x (барлық басылымдары) 64-биттік; Postgres Pro 15.x (барлық басылымдары) 64-биттік; Postgres Pro 15.x 64-биттік (Corosync/Pacemaker кластері); Postgres Pro 16.x (барлық басылымдары) 64-биттік; Postgres Pro 16.x Enterprise 64-биттік (Built-in High Availability кластері); Postgres Pro 17 (барлық басылымдары) 64-биттік; Postgres Pro 17 Enterprise 64-биттік (Built-in High Availability кластері); Postgres Pro 18 (барлық басылымдары) 64-биттік; Postgres Pro 18 Enterprise 64-биттік (Built-in High Availability кластері); Platform V Pangolin 6.5.1 64-биттік; Platform V Pangolin 6.5.1 64-биттік (Built-in High Availability кластері); Jatoba 4 64-биттік; Jatoba 5 64-биттік; Tantor SE 1C 64-биттік. Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы тиіс: • антивирустық қорғаныс бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою; • орталықтандырылған теңшеу, әкімшілендіру; • қорғаныс құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау; • саясаттар мен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға кері қайтару мүмкіндігі; • қайта бөлу жүзеге асырылатын триггерлер иерархиясы; • жаңартуларды пайдаланушылардың жұмыс орындарына алынғаннан кейін бірден жеткізу; • желідегі виртуалды машиналарды анықтау және егер бұл машиналар бір физикалық серверде орналасса, олардың арасында

	іске қосылатын тапсырмалардың жүктеме теңгерімін бөлу; • әр деңгейде әкімшілер мен операторлардың құқықтарын, сондай-ақ берілетін есептілік нысандарын теңшеу мүмкіндігі бар көпдеңгейлі басқару жүйесін құру; • кез келген деңгейдегі әкімшілендіру серверлерінің иерархиясын құру және жоғарғы деңгейден бүкіл иерархияны орталықтандырылған басқару мүмкіндігі; • басқару серверлері үшін мультиарендалықты (multi- tenancy) қолдау; • бағдарламалық құралдар мен антивирустық дерекқорларды әртүрлі көздерден, байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да жаңарту; • басқару сервері арқылы антивирустық БЖ өндірушісінің бұлттық серверлеріне қолжетімділік; • клиенттік компьютерлерге лицензияны автоматты түрде тарату; • орнатылған антивирустық қорғаныс қолданбаларының жұмысындағы оқиғалар туралы хабарландыру тетігінің болуы және олар туралы пошта хабарландыруларын жіберуді теңшеу; • антивирустық қорғаныс оқиғалары, орнатылған бағдарламаларды лицензиялау деректері бойынша графикалық есептер құру; • жүйенің жұмысы туралы алдын ала теңшелген стандартты есептердің болуы; • есептерді PDF және XML форматындағы файлдарға экспорттау; • антивирустық бағдарламалық жасақтама орнатылған желінің барлық ресурстары бойынша резервтік қоймалар мен карантин нысандарын орталықтандырылған басқару; • басқару серверінде аутентификациялауға арналған ішкі есептік жазбаларды жасау; • Әкімшілендіру консоліне рұқсатсыз қолжетімділік қаупін азайту үшін екі кезеңдік тексеру; • басқару жүйесінің кірістірілген құралдарымен басқару жүйесінің резервтік көшірмесін жасау; • вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы; • WEB консолін пайдаланып антивирустық қорғанысты басқару; • әкімшілендіру сервері арқылы да, әкімшілендіру серверіне жүктемені азайту және корпоративтік желідегі деректер трафигін оңтайландыру үшін тарату нүктелері арқылы да басқарылатын құрылғылардағы антивирустық дерекқорлар мен бағдарламалық модульдерді жаңарту және тарату; • жүктелетін жаңартуларды басқарылатын құрылғыларға орнатудың алдында олардың жұмысқа қабілеттілігі мен қателердің бар-жоғын жаңартуларды тексеру тапсырмасы арқылы тексеру; • антивирустық дерекқорлар мен бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары функциясын пайдалану; • орталықтандырылған басқару серверлері арасында шифрлау кілттерін беру мүмкіндігі; • негізгі Сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйелері бар Серверлерді бағынышты ретінде басқару; • оқиғалар таңдамаларын экспорттау және импорттау мүмкіндігі; • оқиғаларды CEF немесе LEEF форматтарында SIEM жүйесіне экспорттау мүмкіндігі; • Android және iOS платформаларындағы мобильді құрылғыларды басқару мүмкіндігі; • басқарылатын құрылғыларға орнатылған бағдарламалар туралы ақпарат алу; • Microsoft Windows басқаруындағы пайдаланушылар компьютерлері мен серверлеріндегі орнатылған қолданбалар мен операциялық жүйедегі осалдықтарды автоматтандырылған іздеу және жабу; • Microsoft Active Directory және Samba домен контроллерлері бойынша

	құрылғыларды іздеу мүмкіндігі; • Windows ОЖ басқаруындағы әкімшілендіру серверінен Linux ОЖ басқаруындағы әкімшілендіру серверіне деректерді автоматтандырылған тасымалдау мүмкіндігі; • басқарылатын құрылғыларды қашықтан диагностикалау мүмкіндігі; • кластерлік технологияны қолдау; • басқарылатын құрылғылардан үйлесімсіз БЖ- ны орталықтандырылған түрде жою мүмкіндігі; • басқарылатын құрылғыларды орталықтандырылған түрде қайта жүктеу мүмкіндігі; • автономды пайдаланушылар үшін, олардың орналасқан жеріне байланысты бір немесе әртүрлі орталықтандырылған басқару серверлеріне қосылу үшін Linux құрылғыларымен қосылым профильдерін белгілеу мүмкіндігі; • FreeIPA және ALD Pro домен контроллерлерін қолдау; • Kerberos бойынша домендік аутентификацияны қолдау (жалғыз кіру технологиясы, оның ішінде сертификаттар негізінде). Антивирустық дерекқорларды жаңартуға қойылатын талаптар Жаңартылып отыратын антивирустық дерекқорлар келесі функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс: • күнтізбелік тәулік ішінде кемінде 24 рет антивирустық дерекқорларды жаңарту ережелерін жасау; • жаңартудың бірнеше жолы, оның ішінде байланыс арналары арқылы және ажыратылатын электрондық ақпарат тасығыштарда; • жаңартулардың тұтастығы мен түпнұсқалығын электрондық цифрлық қолтаңба құралдарымен тексеру. Пайдалану құжаттамасына қойылатын талаптар • Антивирустық құралдармен бірге берілетін құжаттама тиісті антивирустық қорғаныс құралын орнату, теңшеу және пайдалану процесін егжей-тегжейлі сипаттауы тиіс. Техникалық қолдауға қойылатын талаптар Антивирустық бағдарламалық жасақтаманың техникалық қолдауы: • Қазақстан Республикасының бүкіл аумағында электрондық пошта арқылы және Интернет арқылы антивирустық қорғаныс құралдары өндірушісінің және оның серіктестерінің сертификатталған мамандары тарапынан орыс тілінде берілуі тиіс. • Антивирустық шешім өндірушісінің веб-сайты орыс тілінде болуы, антивирустық шешімнің техникалық қолдауына арналған арнайы бөлімі, толықтырылып отыратын білім базасы, сондай-ақ бағдарламалық өнімдерді пайдаланушылар форумы болуы тиіс. • 24/7 регламенттелген техникалық қолдау желісінің болуы (бірінші желі жеткізушінің меншікті инженерлерінің күшімен).

Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	Жеткізуші антивирустық бағдарламалық жасақтамаға кемінде 3 (үш) жыл қолданылу мерзімімен лицензиялар беруге міндетті. Көрсетілген мерзімге лицензияларды сатып алуға, ұзартуға және белсендіруге байланысты барлық шығыстар Жеткізушінің ұсынысы құнына енгізілуі тиіс. • Жеткізуші Kaspersky ресми серіктесі мәртебесіне ие болуы тиіс • Жеткізуші жеткізушінің өкілеттіктерін растайтын өндірушінің авторизациялық хатын беруі тиіс.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Департамент полиции Актюбинской области Министерства внутренних дел Республики Казахстан"
Наименование организатора	Государственное учреждение "Департамент полиции Актюбинской области Министерства внутренних дел Республики Казахстан"
№ конкурса:	№ 17952736-1
Наименование конкурса:	Услуги по продлению лицензии антивируса для нужд ДП Актюбинской области.
Номер лота:	№ 82838444-ОК2
Наименование лота:	Услуги по продлению лицензий на право использования программного обеспечения
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	582950.000.000000
Наименование услуги:	Услуги по продлению лицензий на право использования программного обеспечения
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	43756681.03
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	43756681.03
Срок оказания услуги:	16 календарных дней с момента вступления в силу Договора
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	36

Описание требуемых характеристик, параметров и иных исходных данных	Общие требования Антивирусные средства должны включать: » программные средства антивирусной защиты для рабочих станций Windows; для файловых серверов Windows; для рабочих станций Mac; для рабочих станций и серверов Linux; 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; Windows 8 Professional / Enterprise (32 / 64-разрядная); Windows 8.1 Professional / Enterprise (32 / 64-разрядная); Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise/Enterprise multi-session; Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise; 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 MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств; • записи в журнал событий о записи и/или удалении файлов на съемных дисках; • назначение приоритета для правил доступа к устройствам с файловой системой; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защиты от атак типа BadUSB; • 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; Windows MultiPoint Server 2011 (64-разрядная); Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше; Windows Web Server 2008 R2 Service Pack 1 и выше; Windows Server 2012 Foundation / Essentials / Standard / Datacenter (включая режим Server Core); Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (вклDatacenter (включая режим Server Core); Windows Server 2019 Essentials /

	Standard / Datacenter (включая режим Server Core); Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core), 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 работеючая режим Server Core); Windows Server 2016 Essentials / Standard /

	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: o 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 - 7.9.; CentOS Stream 8-10; 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 - 7.9; Oracle Linux 8.5 - 8.9; Oracle Linux 9.4 - 9.6; Red Hat® Enterprise Linux® 7.2 - 7.9.; Red Hat Enterprise Linux 8.5 - 8.9.; Red Hat Enterprise Linux 9.4 - 9.6.; Red Hat Enterprise Linux 10.0, 10.1.; Rocky Linux 8.6 - 8.9.; Rocky Linux 9.4 - 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 - 15.7.; Ubuntu® 22.04 LTS.; Ubuntu 24.04 LTS.; Альт Образование 10, 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: o 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 Android-устройств. 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 MDM-устройств 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; Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSB) 64-разрядная; Windows Server 2019 Standard/Datacenter/Core 64-разрядная; Windows Server 2022 Standard/Datacenter/Core 64-разрядная; Windows Server 2025 Standard/Datacenter/Core 64-разрядная; 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, 7.0; Microsoft Hyper-V Server 2019, 2022 (64-разрядная); Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x.; Parallels Desktop 18.; 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; Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная; Microsoft SQL Server 2019 (все редакции) для Windows/Linux 64-разрядная (требуются дополнительные действия); Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная; MySQL 5.7 Community 32-разрядная/64-разрядная; MySQL 8.0 Community 32-разрядная/64-разрядная; MariaDB 10.5 (сборка 10.5.17 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; Postgres Pro 13.x Windows/Linux 64-разрядная; 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; Debian GNU/Linux 13 (Trixie) 64-разрядная; Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная; 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: o VMware vSphere 6.7.0., 7.0.3; Microsoft Hyper-V Server 2019, 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: o 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 пользователей программных продуктов. • Наличие регламентированной линии технической поддержки 24/7 (первая линия силами собственных инженеров поставщика).
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	Поставщик обязан предоставить лицензии на антивирусное программное обеспечение сроком действия не менее 3 (трех) лет. Все расходы, связанные с приобретением, продлением и активацией лицензий на указанный период, должны быть включены в стоимость предложения Поставщика. • Поставщик должен обладать статусом официального партнера Kaspersky • Поставщик должен предоставить авторизационное письмо от производителя, подтверждающее полномочия поставщика.