Бекітемін
Қарағанды облысы білім басқармасының Қарағанды қаласы
білім бөлімінің «№36 жалпы білім беретін мектебі»КММ
_____ Ракишева Ж.Ж.

1 жыл мерзімге 100 жұмыс станциясы үшін Kaspersky Endpoint бағдарламалық құралын пайдалану құқығына лицензияны жаңарту қызметтерінің техникалық ерекшеліктері

Құқыққа лицензияны ұзарту қызметі
бағдарламалық жасақтаманы пайдалану
"Мемлекеттік сатып алу туралы"Қазақстан Республикасы Заңының 38-бабы 2-тармағының 1-тармағы негізінде.
Негізгі (орнатылған) жабдықты, сондай-ақ орнатылған бағдарламалық қамтамасыз етуді (лицензиялық бағдарламалық қамтамасыз етуді)жинақтау, жаңғырту және жете жарақтандыру үшін:

Бағдарламалық жасақтаманы пайдалану құқығына лицензияны ұзарту
kasperskyendpointsecurityforbusinessselect100 жұмыс станциясында 12 ай қызмет етеді.
Жалпы талаптар
Антивирустық құралдар мыналарды қамтуы керек:
"Windows жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама;
"MacOS жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама;
"жұмыс станциялары мен серверлерге арналған антивирустық бағдарламалық құралlinux;
"Windows файлдық серверлеріне арналған антивирустық бағдарламалық жасақтама;
"мобильді құрылғыларға (смартфондар мен планшеттерге)арналған антивирустық бағдарламалық жасақтама;
"орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары;
"жаңартылатын зиянды бағдарлама қолтаңбасы және шабуыл дерекқорлары;
"пайдалану құжаттамасы орыс тілінде.
Барлық антивирустық құралдардың, соның ішінде басқару құралдарының бағдарламалық интерфейсі орыс және ағылшын тілдерінде болуы керек.
Барлық антивирустық құралдар, соның ішінде басқару элементтері орыс және ағылшын тілдерінде контекстік анықтамалық жүйеге ие болуы керек.
Windows жұмыс станцияларына арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар
Антивирустық қорғаныс бағдарламалық жасақтамасы келесі нұсқалардағы жұмыс станциялары үшін операциялық жүйені басқаратын компьютерлерде жұмыс істеуі керек:
O Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 және одан жоғары;
O Windows 8 Professional / Enterprise (32 / 64 бит);
O Windows 8.1 Professional / Enterprise (32 / 64 бит);
O Windows 10 Home / Pro / Pro жұмыс станциялары / Education / Enterprise;
O Windows 11 Home / Pro / Pro жұмыс станциялары / Education / Enterprise.

- Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек:
- * нақты уақыт режимінде және нысанның мәтінмәндік мәзірінен сұраныс бойынша антивирустық сканерлеу;
- * кесте бойынша антивирустық сканерлеу;
- * қосылатын құрылғыларды антивирустық сканерлеу;
- * бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;

- * белсенді инфекцияның әрекеттерін бейтараптандыру;
- * қолданбаның мінез-құлқын және оның зиянды әрекеттерін анықтау және рұқсат етілмеген әрекеттерді анықтау үшін жүйеде жасаған әрекеттерін талдау;
- * желі арқылы қол жетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қоңырауларды талдау;
- * бағдарламалық жасақтамадағы осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, соның ішінде жүйелік процестердің жадын қорғау;
- * емдеу кезінде зиянды бағдарламалық қамтамасыз ету әрекеттерін кері қайтару, оның ішінде шифрланған, зиянды бағдарламалармен, файлдармен қалпына келтіру;
- * артықшылық шектеулері (тізілімге жазылу, файлдарға, қалталарға және басқа процестерге қол жеткізу, тапсырмаларды жоспарлаушыға хабарласу, құрылғыларға қол жеткізу, объектілерге құқықтарды өзгерту және т. б.) процестер мен қосымшалар үшін, сенім деңгейін анықтай отырып, динамикалық түрде жаңартылатын теңшелетін қолданбалар тізімдері;
- * іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау;
- * келесі форматтағы мұрағаттардағы файлдарды антивирустық тексеру және емдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- * келесі хаттамалар бойынша берілетін кіріс және шығыс трафикті тексеретін зиянды бағдарламалардан электрондық поштаны қорғау: IMAP, SMTP, POP3, MAPI, NNTP;
- * берілген файл түрлерінің атын өзгерту немесе жою мүмкіндігі бар пошта тіркемелерінің сүзгісі;
- * https (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP хаттамалары бойынша пайдаланушының компьютеріне келіп түсетін желілік трафикті, оның ішінде эвристикалық талдау, сенімді ресурстарды теңшеу мүмкіндігі және құлыптау немесе статистика режимінде жұмыс істеу арқылы тексеру;
- * жүктелетін веб-беттердегі баннерлер мен қалқымалы терезелерді бұғаттау;
- * фишингтік және қауіпті сайттарды тану және бұғаттау;
- * желілік сегменттерді санаттау мүмкіндігі бар бағдарламалар үшін желілік пакеттік ережелер мен желілік ережелерді құруға мүмкіндік беретін кіріктірілген желі экраны;
- * кез-келген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран ережелерін қолдана отырып, желілік шабуылдардан қорғау;
- * құрылғының MAC мекенжайын қолдан жасау үшін ARP протоколындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
- * бірнеше желілік қосылымдарды бір уақытта орнатуды бұғаттау мүмкіндігі бар желілік көпір түріндегі желілік қосылымдарды басқару;
- * барлық немесе белгілі бір пайдаланушы топтары (ActiveDirectory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелер жасау, компонент бағдарламаны, метадеректерді, сертификатты немесе оның ізін, бақылау сомасын табу жолында да, өндіруші ұсынған алдын ала белгіленген қолданба санаттары бойынша да қолданбаларды бақылауы керек бағдарламалық жасақтама, компонент қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе құлыптау режимінде жұмыс істеуі керек;
- * құрылғының түрі және / немесе пайдаланылатын автобус бойынша сыртқы енгізу/шығару құрылғыларымен пайдаланушының жұмысын бақылау, олардың идентификаторы бойынша сенімді құрылғылардың тізімін жасау мүмкіндігі және ActiveDirectory ішінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігі;

- * MTP құрылғыларын басқару және құрылғыларды бақылау шеңберінде барлық немесе пайдаланушылар топтары (ActiveDirectory немесе жергілікті пайдаланушылар/топтар) үшін осы типтегі құрылғыларға қол жеткізу ережелерін теңшеу;
- * алынбалы дискілердегі файлдарды жазу және / немесе жою туралы Оқиғалар журналына жазбалар;
- * файлдық жүйесі бар құрылғыларға қол жеткізу ережелеріне басымдық беру;
- * пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық жаңартылған санатқа, сондай-ақ ақпарат түріне (аудио, видео және т. б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге мүмкіндік беру, сондай-ақ оны тек белгілі бір пайдаланушыларға тағайындау. ActiveDirectory;
- * BadUSB типті шабуылдардан қорғау;
- * анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтауға арналған арнайы тапсырманы іске қосыңыз.
- * қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ пароль арқылы қолданба параметрлеріне кіруді қорғау;
- * сенімді қашықтан басқару бағдарламалары арқылы параметрлерді басқару;
- * тек таңдалған антивирустық бағдарламалық құрал компоненттерін орнату;
- * бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
- * тапсырмаларды кесте бойынша және/немесе қолданбаны іске қосқаннан кейін бірден іске қосыңыз;
- * файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- * өткен тексеру уақытынан бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- * антивирустық бағдарламаның тұтастығын тексеру;
- * файлдың бақылау сомасы, аты/каталог маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу;
- * ережелер мен ерекшеліктер тізімін XML форматына импорттау және экспорттау;
- * антивируста жойылған вирус жұққан файлдар үшін қорғалған сақтау орны бар, оларды қалпына келтіру мүмкіндігі бар;
- * антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы;
- * антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ Графикалық интерфейстің жеңілдетілген нұсқасының болуы, мүмкіндіктердің минималды жиынтығы;
- * Интеграцияwindows Defender Security Center;
- * Antimalware Scan Interface (AMSI)қолдауының болуы;
- * Linux үшін Windows Subsystem (WSL)қолдауының болуы;
- * резервтік қоймадан объектілерді қалпына келтіруді құпия сөзбен қорғаңыз;
- * интернет байланысы шектеулі болған жағдайда желілік трафиктің шектеулері;
- * TCP және UDP хаттамалары бойынша желіні бақылау құралының болуы;
- * тексеру үзілген жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;
- * орнату мүмкіндігі тапсырманың орындалу ұзақтығын шектеу;
- * тексеру тапсырмаларын кезекке қою мүмкіндігі, егер тексеру қазірдің өзінде орындалса.
- Windows серверлеріне арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар
- Антивирустық бағдарламалық жасақтама келесі нұсқалардың файлдық серверлері үшін операциялық жүйені басқаратын компьютерлерде жұмыс істеуі керек:

- O Windows Small Business Server 2011 Essentials / Standard (64 биттік), Microsoft Small Business Server 2011 Standard (64 биттік) Қолдайдыmicrosoft Windows Server 2008 R2 үшін Service Pack 1 орнатылған;
- O Windows MultiPoint Server 2011 (64 бит);
- O Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 және одан жоғары;
- o Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- o Windows Server 2016 Essentials / Standard / Datacenter;
- o Windows Server 2019 Essentials / Standard / Datacenter;
- o Windows Server 2022.
-
- Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек:
- * нақты уақыт режимінде және нысанның мәтінмәндік мәзірінен сұраныс бойынша антивирустық сканерлеу;
- * кесте бойынша антивирустық сканерлеу;
- * қосылатын құрылғыларды антивирустық сканерлеу;
- * бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- * белсенді инфекцияның әрекеттерін бейтараптандыру;
- * қолданбаның мінез-құлқын және оның зиянды әрекеттерін анықтау және рұқсат етілмеген әрекеттерді анықтау үшін жүйеде жасаған әрекеттерін талдау;
- * желі арқылы қол жетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қоңырауларды талдау;
- * бағдарламалық жасақтамадағы осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, соның ішінде жүйелік процестердің жадын қорғау;
- * емдеу кезінде зиянды бағдарламалық қамтамасыз ету әрекеттерін кері қайтару, оның ішінде шифрланған, зиянды бағдарламалармен, файлдармен қалпына келтіру;

* бұлтқа негізделген жаңа қауіптерден қорғау, нақты уақыт режимінде бағдарламаға немесе файлға қатысты үкім шығару үшін өндірушінің ресурстарына қол жеткізуге мүмкіндік береді;
* RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматтарындағы файлдарды антивирустық тексеру және емдеу;
* желілік сегменттерді санаттау мүмкіндігі бар бағдарламалар үшін желілік пакеттік ережелер мен желілік ережелерді құруға мүмкіндік беретін кіріктірілген желі экраны;
* құрылғының MAC мекенжайын қолдан жасау үшін ARP протоколындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
* анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтауға арналған арнайы тапсырманы іске қосыңыз.
* қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалардан, зиянкестерден немесе біліктілігі жоқ пайдаланушылардан қорғауды өшірмеу үшін пароль арқылы қолданба параметрлеріне кіруді қорғау;
* тек таңдалған антивирустық бағдарламалық құрал компоненттерін орнату;
* бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
* тапсырмаларды кесте бойынша және/немесе амалдық жүйе жүктелгеннен кейін бірден іске қосыңыз;
* файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;

* өткен тексеру уақытынан бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету;
* антивирустық бағдарламаның тұтастығын тексеру;
* файлдың бақылау сомасы, аты/каталог маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу;
* антивируста жойылған вирус жұққан файлдар үшін қорғалған сақтау орны бар, оларды қалпына келтіру мүмкіндігі бар;
* антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы;
* антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ Графикалық интерфейстің жеңілдетілген нұсқасының болуы, мүмкіндіктердің минималды жиынтығы;
* Интеграцияwindows Defender Security Center;
* Antimalware Scan Interface (AMSI)қолдауының болуы;
* Linux үшін Windows Subsystem (WSL)қолдауының болуы;
* резервтік қоймадан объектілерді қалпына келтіруді құпия сөзбен қорғаңыз.
* ережелер мен ерекшеліктер тізімін XML форматына импорттау және экспорттау;
* интернет байланысы шектеулі болған жағдайда желілік трафиктің шектеулері;
* тексеру үзілген жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;
* тапсырманың орындалу ұзақтығын шектеу мүмкіндігі;
* тексеру тапсырмаларын кезекке қою мүмкіндігі, егер тексеру қазірдің өзінде орындалса.

- **Мас жұмыс станцияларына арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар**
- **Мас жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:**
- **o macOS 10.14 - 12;**
- **Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек:**
- *** резиденттік антивирустық бақылау;**
- *** бұлтқа негізделген жаңа қауіптерден қорғау, нақты уақыт режимінде бағдарламаға немесе файлға қатысты үкім шығару үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік береді;**
- *** кесте бойынша антивирустық базаларды автоматты түрде жаңарту;**
- *** қалпына келтіру мүмкіндігі үшін вирус жұққан файлдарды жоймас бұрын олардың сақтық көшірмесін жасаңыз;**
- *** бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;**
- *** кез-келген типтегі есептеу желілерінде, соның ішінде сымсыз желілерде жұмыс істеу кезінде ең танымал қосымшаларға арналған кіруді анықтау және алдын-алу жүйесін (IDS/IPS) және желілік белсенділік ережелерін қолдана отырып, желілік шабуылдардан қорғау;**
- *** антивирустық қорғаныс өндірушісінің беделді бұлтты қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды бұғаттау;**
- *** Safari, GoogleChrome және Firefox браузерлері арқылы берілетін желілік трафикті тексеру (HTTP және HTTPS трафигі);**
- *** пайдаланушының Интернет желісімен жұмысын бақылау, соның ішінде санаттарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартылған белгілі бір ресурстарға немесе ресурстар санаттарына кіруге нақты тыйым салуды немесе рұқсатты қосу**

- *** өткен тексеру уақытынан бері күйі өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету;**
- *** бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;**
- *** жаңа kav пәрменін пайдаланып пәрмен жолынан кеңейтімдерді орнату мүмкіндігі;**
- *** файлдық операцияларды ұстап қалу деңгейінде көрсетілген аймақтарды тексеру кезінде ерекшеліктерді орнату мүмкіндігі;**
- *** дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнату мүмкіндігі.**
-
- **Жұмыс станциялары мен серверлерге арналған антивирустық бағдарламалық құралға қойылатын талаптарlinux**
- **Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың 32 биттік операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:**
- **o CentOS 6.7 және одан жоғары.**
- **o Debian GNU / Linux 10.1 және одан жоғары.**
- o Debian GNU/Linux 11.
- o Mageia 4.
- O Red Hat Enterprise Linux 6.7 және одан жоғары.
- O Alt 8 SP жұмыс станциясы.
- O Alt 8 SP сервері.
- O АльтОбразование 10.
- o АльтРабочаяСтанция 10.
- Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың 64 биттік операциялық жүйелерімен жұмыс істейтін компьютерлерде жұмыс істеуі керек:
- O AlmaLinux OS 8 және одан жоғары.
- O AlmaLinux OS 9 және одан жоғары.
- O AlterOS 7.5 және одан жоғары.
- o Amazon Linux 2.
- o Astra Linux Common Edition 2.12.
- o Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.5).
- o Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.6).
- o Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.7).
- o ASTRALINUXSPECIALEDITION РУСБ.10015-16 (орындау 1) (кезекті жаңарту 1.6).
- o CentOS 6.7 және одан жоғары.
- o CentOS 7.2 және одан жоғары.
- o CentOS Stream 9.
- o Debian GNU / Linux 10.1 және одан жоғары.
- o Debian GNU/Linux 11.
- o EMIAS 1.0.
- o EulerOS 2.0 SP5.
- O LinuxMint 19.2 және одан жоғары.
- O LinuxMint 20.3 және одан жоғары.
- o openSUSE Leap 15.0 және одан жоғары.
- o Linacle Linux 7.3 және одан жоғары.
- o Linacle Linux 8.0 және одан жоғары.

    - O Red Hat Enterprise Linux 6.7 және одан жоғары.
    - O Red Hat Enterprise Linux 7.2 және одан жоғары.
    - O Red Hat Enterprise Linux 8.0 және одан жоғары.
    - o Red Hat Enterprise Linux 9.
    - O Rocky Linux 8.5 және одан жоғары.
    - O SUSE Linux Enterprise Server 12.5 және одан жоғары.
    - O SUSE Linux Enterprise Server 15 және одан жоғары.
    - o Ubuntu 20.04 LTS.
    - o Ubuntu 22.04 LTS.
    - O Alt 8 SP жұмыс станциясы.
    - O Alt 8 SP сервері.
    - O АльтОбразование 10.
    - o АльтРабочаяСтанция 10.
    - O АльтСервер 10.
    - O Атлант, Alcyone құрастыру, 2022.02 нұсқасы.
    - o Goslinux 7.17.
    - o Goslinux 7.2.
- o red OS 7.3.
- o шық "Кобальт" 7.9.
- o шық "Хром" 12.
- O ОСОН "негіз".
- ARM архитектурасына арналған 64 биттік операциялық жүйелер:
- o ASTRALINUXSPECIALEDITION РУСБ.10152-02(кезекті жаңарту 4.7).
- o EulerOS 2.0 SP8.
- o SUSE Linux Enterprise Server 15 SP3.
- o Ubuntu 20.04 LTS.
- O Alt 8 SP сервері.
- o red OS 7.3.
- Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек:
- * резиденттік антивирустық мониторинг;
- * нақты уақыт режимінде іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау;
- * SMB / NFS арқылы қол жетімді ресурстарды тексеру;
- * ядро жадын тексеру мүмкіндігі;
- * бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- * пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу;
- * zip мұрағаттарындағы файлдарды антивирустық тексеру; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
- * мәтіндік форматтағы электрондық пошта хабарламаларын тексеру (Plaintext);
- * файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытының шегі, тексерілетін файл өлшемінің шегі, кэштеу механизмі тексерілген және тексерілгеннен кейін өзгертілмеген файлдар туралы ақпарат);
- * SMB / NFS протоколдары бойынша желіге қол жетімді жергілікті каталогтардағы файлдарды қашықтан зиянды шифрлаудан қорғау;
- * тексеру кезінде файлдарды бұғаттау опциясын қосыңыз;
- * күдікті және бүлінген объектілерді карантинге орналастыру;

- * SAMBA деңгейіндегі файлдық операцияларды ұстап алу және тексеру;
- * ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару;
- * тапсырмаларды кесте бойынша және/немесе амалдық жүйе жүктелгеннен кейін бірден іске қосыңыз;
- * есептерді HTML және CSV форматтарында экспорттау және сақтау;
- * файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін ДК ресурстарын пайдалануды икемді басқару;
- * жұқтырған объектінің көшірмесін, егер ол ақпараттық құндылықты білдірсе, талап бойынша Объектіні ықтимал қалпына келтіру мақсатында емдеу және жою алдында резервтік қоймада сақтау;
- * түбірлік құқықтары жоқ пайдаланушы графикалық интерфейсі арқылы басқару;
- * жоғарыда аталған барлық компоненттерді бірыңғай басқару жүйесі немесе веб-консоль арқылы орталықтандырылған басқару;
    - • 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
    - • HTTP/HTTPS және FTP протоколдары арқылы пайдаланушының компьютеріне келетін трафикті, сондай-ақ веб-мекенжайлардың зиянды немесе фишингтік мекенжайларға қатыстылығын орнату мүмкіндігін тексеру;
    - • получения данных о действиях программ на компьютере пользователя;
    - • создание файлов трассировки при запуске программы;
    - • получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
    - • проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;
    - • сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий.
    -
    - Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін антивирустық қорғаудың бағдарламалық құралдарына қойылатын талаптар
    - Windows файлдық серверлеріне арналған антивирустық бағдарламалық қамтамасыз ету келесі нұсқалардың операциялық жүйелерімен жұмыс істейтін компьютерлерде жұмыс істеуі керек:
    - Microsoft Windows 32 биттік операциялық жүйелері
    - o WINDOWS Server 2003 Standard / Enterprise / Datacenter SP2 жаңарту бумасымен немесежоғарыда;
    - o Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 жаңарту бумасымен немесежоғарыда;
    - o WINDOWS Server 2008 Standard / Enterprise / Datacenter SP2 жаңарту бумасымен немесежоғарыда;
    - o WINDOWS Server 2008 Core Standard / Enterprise / Datacenter SP2 жаңарту бумасымен немесежоғары.
    - 64 биттік Microsoft Windows операциялық жүйелері
    - o WINDOWS Server 2003 Standard / Enterprise / Datacenter SP2 жаңарту бумасымен немесежоғарыда;
    - o Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 жаңарту бумасымен немесежоғары;

- o WINDOWS Server 2008 Core Standard / Enterprise / Datacenter SP2 жаңарту бумасымен немесежоғары;
- o WINDOWS Server 2008 Standard / Enterprise / Datacenter SP2 жаңарту бумасымен немесежоғары;
- o Microsoft Small Business Server 2008 Standard / Premium SP2 немесежоғары;
- o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 жаңарту бумасымен немесежоғарыда;
- o Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 жаңарту бумасымен немесежоғары;
- o WindowsHyper-vserver 2008 r2 sp1 немесе одан жоғары жаңарту бумасымен;
- o Microsoft Small Business Server 2011 Essentials / Standard SP1 немесежоғарыда;

- o Microsoft Windows MultiPoint Server 2011 Standard / Premium;
- o Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- o Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
- o Microsoft MultiPoint Server 2012 Standard / Premium;
- o Windows Storage Server 2012;
- o Windows Hyper-V Server 2012;
- o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- o Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
- o Windows Storage Server 2012 R2;
- o Windows Hyper-V Server 2012 R2;
- o Windows Server 2016 Essentials / Standard / Datacenter;
- o Windows Server 2016 MultiPoint;
- o Windows Server 2016 Core Standard / Datacenter;
- o Microsoft Windows MultiPoint Server 2016;
- o Windows Storage Server 2016;
- o Windows Hyper-V Server 2016;
- o Windows Server 2019 Essentials / Standard / Datacenter;
- o Windows Server 2019 Core;
- o Windows Storage Server 2019;
- o Windows Hyper-V Server 2019;
- o Windows Server 2022;
- o Windows 10 Enterprise multi-session.
- Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек:
- * нақты уақыт режимінде және сұраныс бойынша әртүрлі функцияларды орындайтын серверлерде антивирустық сканерлеу: терминал серверлері, баспа серверлері, қолданба серверлері және домен контроллері, файл серверлері;
- * пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу;
- * тапсырмаларды кесте бойынша және/немесе амалдық жүйе жүктелгеннен кейін бірден іске қосыңыз;
- * бұлтқа негізделген жаңа қауіптерден қорғау, нақты уақыт режимінде бағдарламаға немесе файлға қатысты үкім шығару үшін өндірушінің арнайы сайттарына жүгінуге мүмкіндік береді;
- * RAR, ARJ, ZIP, CAB форматтарындағы файлдарды антивирустық тексеру және емдеу;
- * файлдарды қорғау, балама файлдық жүйелер ағындары (NTFS-streams), жүктеу жазбасы, жергілікті және алынбалы дискілердің жүктеу секторлары;
- * MicrosoftWindowsScriptTechnologies (немесе ActiveScripting) технологиялары бойынша жасалған VBScript және JScript сценарийлерінің қорғалған серверінде орындау әрекеттерін

үздіксіз қадағалау, сценарийлердің бағдарламалық кодын тексеру және қауіпті деп танылғандардың орындалуына автоматты түрде тыйым салу.

- * желі арқылы қол жетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қоңырауларды талдау;
- * MicrosoftWindows контейнерлерін тексеру;
- * процесс жадындағы осалдықтарды пайдаланудан қорғау;
- * бұзылған процестерді автоматты түрде аяқтау мүмкіндігі болуы керек, ал маңызды жүйелік процестер аяқталмауы керек;
- * қорғалған тізімге процестерді қосыңыз;
- * өткен тексеру уақытынан бері күйі өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- * жеке модульдерді жеке тапсырма арқылы олардың тұтастығын бұзуға тексеру;
- * жеке тапсырма ретінде сервердің маңызды аймақтарын тексеру параметрлері;
- * тапсырмалардың басымдылығына байланысты сервер ресурстарын антивирус пен басқа қосымшалар арасында бөлуді реттеу;
- * фонда антивирустық сканерлеуді жалғастыру;
- * маңызды оқиғалар туралы әкімшілерге хабарлаудың бірнеше жолдарының болуы (пошта хабарламасы, дыбыстық ескерту, қалқымалы терезе, Оқиғалар журналына жазу);
- * зиянды бағдарламалардан, зиянкестерден немесе біліктілігі жоқ пайдаланушылардан қорғауды өшірмеуге мүмкіндік беретін, сондай-ақ антивирусты басқаруға тыйым салатын немесе рұқсат беретін рұқсат тізімдері арқылы қолданба мен қызмет опцияларына рөлдік қол жеткізу;
- * Siem жүйелерімен интеграция;
- * антивирустың жұмыс процестерінің санын қолмен көрсету;
- * графикалық интерфейсті өшіру;
- * қашықтан және жергілікті басқару консолінің болуы;
- * пәрмен жолынан антивирус параметрлерін басқару;
- * бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
- * ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару;
- * желілік шабуылдардың белгілері үшін кіріс трафигін талдауды қамтамасыз ететін желілік қауіптерден қорғау;
- * бағдарлама процестерін сыртқы қауіптерден қорғауды қосыңыз немесе өшіріңіз (әдепкі бойынша функция қосылады). Функция қосылған кезде бағдарлама өзінің процестерін, сондай-ақ әкімшілік агенттің процестерін үшінші тарап процестерінің араласуынан қорғайды.
- Мобильді құрылғыларды антивирустық қорғау бағдарламалық құралдарына қойылатын талаптар
- Смартфондарды антивирустық қорғауға арналған бағдарламалық жасақтама келесі мобильді ОЖ - де жұмыс істеуі керек:
- o Android 5.0–13 (Go Edition қоспағанда, Android 12L қоса алғанда);
- o iOS 10-16 немесе iPadOS 13-15;
- Android ОЖ үшін смартфондарды антивирустық қорғау бағдарламалық құралында келесі функциялар іске асырылуы керек:
- * смартфонның файлдық жүйесін тұрақты антивирустық қорғау, антивирустық қорғаныс өндірушісінің бұлтқа негізделген беделді қызметін қолдана отырып, қосымша тексеру деңгейімен;
    - * құрылғының файлдық жүйесін сұраныс бойынша және кесте бойынша тексеру;
    - * орнатылған қолданбаларды жылдам тексеру

- * антивирустық қорғаныс құралдарын өндірушінің беделді бұлтты қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды бұғаттау;
- * жұқтырған объектілерді оқшаулауға арналған қойманың болуы;
- * зиянды бағдарламаларды іздеу және қауіпті объектілерді жою кезінде қолданылатын антивирустық базаларды кесте бойынша жаңарту;
- * көрсетілген қолданбаларды, соның ішінде алдын ала белгіленген қолданба санаттарын пайдаланып іске қосуды блоктау;
- * рұқсат етілген қолданбалардың ақ тізімдерін қолдау;
- * қосымшалардың іске қосылуын бақылау шеңберінде жүйелік қосымшаларды бұғаттау;
- * FirebaseCloudMessaging (FCM)қызметі арқылы командалар мен хабарландыруларды жіберу;
- * Wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануға тыйым салу;
- * Wi-Fi желілеріне қосылу параметрлерін көрсетіңіз;
- * орнатуға міндетті қосымшаларды көрсетіңіз;
- * мобильді құрылғыны құлыптау, деректерді жою, жұмысқа байланысты деректерді жою, құрылғының орналасқан жерінің координаттарын алу, зауыттық параметрлерге қашықтан оралу (factoryreset);
- * қағидалар тізімін құру, олардың негізінде мобильді құрылғының құрылғыны автоматты түрде бұғаттау, деректерді жою, сәйкессіздіктер анықталған кезде корпоративтік қосымшаларды іске қосуға тыйым салу мүмкіндігімен корпоративтік саясатқа сәйкестігін тексеру жүзеге асырылатын болады;
- * Samsung knox1 және knox2 технологияларын қолдау.
- AppleiOS ОЖ үшін смартфондарды қорғау бағдарламалық құралында келесі функционалдылықтар іске асырылуы керек:
- * топтық саясаттарды қолдана отырып, IOS MDM құрылғыларының параметрлерін қашықтан конфигурациялау;
- * деректерді блоктау және жою пәрменін жіберу;
- * мобильді құрылғылардың топтық қауіпсіздік саясатын жасаңыз;
- * ExchangeActiveSync\ iOS MDM протоколы арқылы қосылған құрылғылардың конфигурация параметрлерін қашықтан реттеңіз;
- * пайдаланушылардың мобильді құрылғыларының жұмысы туралы есептер мен статистиканы алу;
- * supervisedmode пайдалану кезінде антивирустық қорғаныс өндірушісінің беделді бұлттық қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды бұғаттау;
- * бір басқару консолі арқылы орталықтандырылған басқару;
- * басқарылатын құрылғыда ITUNES, Safari немесе GameCenter сияқты құрылғының жергілікті қосымшаларын пайдалануға болатындығын басқаруға мүмкіндік беретін компоненттің болуы.
- Windows ОЖ негізіндегі орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдарына қойылатын талаптар
- Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:
- o Microsoft Windows 10 Enterprise 2015 ltsb 32 биттік / 64 биттік;
- o Microsoft Windows 10 Enterprise 2016 ltsb 32 биттік / 64 биттік;
- o Microsoft Windows 10 Enterprise 2019 ltsc 32 биттік / 64 биттік;
- o Microsoft Windows 10 Pro RS5 (қазан 2018 жаңарту, 1809) 32 бит / 64 бит;
- o Microsoft Windows 10 Pro RS5 жұмыс станциялары үшін (Қазан 2018 жаңарту, 1809) 32 бит / 64 бит;
- o Microsoft Windows 10 Enterprise RS5 (қазан 2018 жаңарту, 1809) 32 биттік / 64 биттік;

- o Microsoft Windows 10 Education RS5 (қазан 2018 жаңарту, 1809) 32 биттік / 64 биттік;
- o Microsoft Windows 10 Pro 19H1 32 биттік / 64 биттік;
- O MicrosoftWindows 10 Pro 19h1 жұмыс станциялары үшін 32 бит / 64 бит;
- o Microsoft Windows 10 Enterprise 19h1 32 биттік / 64 биттік;
- o Microsoft Windows 10 Education 19h1 32 биттік / 64 биттік;
- o Microsoft Windows 10 Pro 19H2 32 биттік / 64 биттік;
- O MicrosoftWindows 10 Pro 19h2 жұмыс станциялары үшін 32 бит / 64 бит;
- o Microsoft Windows 10 Enterprise 19H2 32 биттік / 64 биттік;
- o Microsoft Windows 10 Education 19h2 32 биттік / 64 биттік;
- o Microsoft Windows 10 Home 20H1 (мамыр 2020 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Pro 20H1 (мамыр 2020 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Enterprise 20H1 (мамыр 2020 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Education 20H1 (мамыр 2020 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Home 20H2 (қазан 2020 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Pro 20H2 (қазан 2020 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Enterprise 20H2 (қазан 2020 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Education 20H2 (қазан 2020 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Home 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Pro 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Enterprise 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Education 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Home 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Pro 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Enterprise 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит;
- o Microsoft Windows 10 Education 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит;
- O MicrosoftWindows 11 Home 64 биттік;
- O MicrosoftWindows 11 Pro 64 биттік;
- O MicrosoftWindows 11 Enterprise 64 биттік;
- O MicrosoftWindows 11 Education 64 биттік;
- o Microsoft Windows 8.1 Pro 32 биттік/64 биттік;
- o Microsoft Windows 8.1 Enterprise 32 биттік / 64 биттік;
- o Microsoft Windows 8 Pro 32 биттік/64 биттік;
- o Microsoft Windows 8 Enterprise 32 биттік / 64 биттік;
- o Microsoft Windows 7 Professional Service Pack 1 32 бит / 64 бит;
- o Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32 бит / 64 бит;
- O Windows Server 2008 R2 with Standard Service Pack 1 және64 биттен жоғары;
- O Windows Server 2008 R2 Service Pack 1 (қайта қарау) 64 бит;
- O Windows Server 2012 Server Core 64 биттік;
- O WindowsServer 2012 Datacenter 64 биттік;
- O WindowsServer 2012 essentials 64 биттік;
- O WindowsServer 2012 foundation 64 биттік;
- O WindowsServer 2012 standard 64 биттік;
- O Windows Server 2012 R2 Server Core 64 биттік;
- O Windows Server 2012 R2 Datacenter 64 биттік;
- O Windows Server 2012 R2 Essentials 64 биттік;
- O Windows Server 2012 R2 foundation 64 биттік;
- O Windows Server 2012 R2 standard 64 биттік;
- O Windows Server 2016 Datacenter (LTSB) 64 биттік;
- O Windows Server 2016 Standard (LTSB) 64 биттік;
- O Windows Server 2016 (Server Core орнату опциялары) (LTSB) 64 бит;

- O WindowsServer 2019 standard 64 биттік;
- O WindowsServer 2019 Datacenter 64 биттік;
- O WindowsServer 2019 Core 64 биттік;
- O WindowsServer 2022 standard 64 биттік;

- O WindowsServer 2022 Datacenter 64 биттік;
- O WindowsServer 2022 Core 64 биттік;
- O WindowsStorageServer 2012 64 бит;
- O Windows Storage Server 2012 R2 64 бит;
- O WindowsStorageServer 2016 64 бит;
- O WindowsStorageServer 2019 64 биттік.
- Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек:
- o VMwarevSphere 6.7;
- o VMwarevSphere 7.0;
- o VMwareWorkstation 16 Pro;
- o Microsoft Hyper - V Server 2012 64 бит;
- o Microsoft Hyper - V Server 2012 R2 64 бит;
- o Microsoft Hyper - V Server 2016 64 бит;
- o Microsoft Hyper - V Server 2019 64 бит;
- o Microsoft Hyper - V Server 2022 64 бит;
- o CitrixXenServer 7.1 LTSR;
- o CitrixXenServer 8.x;
- o ParallelsDesktop 17;
- o Oracle VM VirtualBox 6.x.
- Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі керек:
- o Microsoft SQL Server 2012 express 64 биттік;
- o Microsoft SQL Server 2014 express 64 биттік;
- o Microsoft SQL Server 2016 express 64 биттік;
- o Microsoft SQL Server 2017 express 64 биттік;
- o Microsoft SQL Server 2019 express 64 биттік;
- o Microsoft SQL Server 2014 (барлық басылымдар) 64 бит;
- o Microsoft SQL Server 2016 (Барлық басылымдар) 64 бит;
- o Microsoft SQL Server 2017 (барлық басылымдар) Windows 64 биттік;
- o Microsoft SQL Server 2017 (барлық басылымдар) Linux үшін 64 бит;
- o Microsoft SQL Server 2019 (барлық басылымдар) Windows 64 биттік (қосымша қадамдар қажет);
- o Microsoft SQL Server 2019 (барлық басылымдар) Linux үшін 64 биттік (қосымша қадамдар қажет);
- o MicrosoftAzure SQL Database;
- O Amazon RDS және MicrosoftAzure бұлттық платформаларында қолдау көрсетілетін SQL серверлерінің барлық нұсқалары;
- o MySQL 5.7 Community 32 биттік / 64 биттік;
- o MySQLStandardEdition 8.0 (8.0.20 және одан жоғары шығарылым) 32 бит / 64 бит;
- o MySQLEnterpriseEdition 8.0 (8.0.20 және одан жоғары шығарылым) 32 бит / 64 бит;
- o MariaDB 10.5.x 32 бит / 64 бит;
- o MariaDB 10.4.x 32 бит / 64 бит;
- o MariaDB 10.3.22 және одан жоғары 32 биттік/64 биттік;
- o MariaDBServer 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік;
- o MariaDBGaleraCluster 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік;
- o MariaDB 10.1.30 және одан жоғары 32 биттік/64 биттік.
- Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек:

- * қорғалатын түйіндер санына байланысты орталықтандырылған басқару, бақылау және жаңарту қондырғысының архитектурасын таңдау;
- * ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында ActiveDirectory-дан ақпаратты оқу;
- * анықталған компьютерлерді IP мекен-жайы, ОЖ түрі, OU AD-да болу ережелерінің параметрлері;
- * желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтары бойынша автоматты түрде бөлу; IP мекенжайы, ОЖ типі, ou AD-да болу бойынша тасымалдау ережелерін теңшеу мүмкіндігі;
- * орталықтандырылған антивирустық бағдарламалық жасақтаманы орнату, жаңарту және жою;
- * орталықтандырылған орнату, әкімшілік;
- * қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау;
- * басқару орталығы құралдарымен үйлеспейтін қосымшаларды орталықтандырылған жою (қолмен және автоматты) ;
- * саясат пен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;
- * антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін-RPC, GPO, басқару жүйесінің құралдары, жергілікті орнату үшін-дербес орнату пакетін құру мүмкіндігі;
- * пайдаланушы кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты антивирустық шешімнің параметрлерін қайта анықтайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар;
- * қайта бөлу орын алатын триггерлердің иерархиялары;
- * клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу;
- * жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
- * виртуалды машиналар желісін тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу;
- * әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігімен көп деңгейлі басқару жүйесін құру;
- * еркін деңгейдегі басқару серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
- * басқару серверлері үшін көп жалға алуды қолдау (multi-tenancy) ;
- * байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту;
- * басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қол жеткізу;
- * клиенттік компьютерлерге лицензияны автоматты түрде тарату;
- * пайдаланушылардың компьютерлерінде орнатылған бағдарламалық жасақтама мен жабдықты түгендеу;
- * орнатылған антивирустық қорғау Қосымшаларының жұмысында оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді баптау;
    - * exchangeactivesync сервері арқылы мобильді құрылғыларды басқару функциясы;
    - * iOS MDM сервері арқылы мобильді құрылғыларды басқару мүмкіндігі;
    - * берілген оқиғалар туралы SMS-хабарламаларды жіберу;
    - * басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату;

- * басқару жүйесіне желілік жүктемені азайту үшін кез-келген ұйымның компьютерін жаңартуларды қайта жіберу орталығына бағыттау;
- * ұйымның кез-келген компьютерін антивирустық агенттердің оқиғаларын бағыттау орталығы, клиенттік компьютерлердің таңдалған тобы, басқару жүйесіне желілік жүктемені азайту үшін орталықтандырылған басқару серверіне бағыттау;
- * вирусқа қарсы қорғау оқиғалары, түгендеу деректері, белгіленген бағдарламаларды лицензиялау деректері бойынша графикалық есептерді құру;
- * жүйенің жұмысы туралы алдын ала конфигурацияланған стандартты есептердің болуы;
- * есептерді PDF және XML форматындағы файлдарға экспорттау;
- * антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин объектілерін орталықтандырылған басқару;
- * басқару серверінде аутентификация үшін ішкі есептік жазбаларды құру;
- * басқару жүйесінің кірістірілген құралдарын басқару жүйесінің сақтық көшірмесін жасау;
- * Windows Failover Clustering қолдауы;
- * Certificate Authority қызметімен Windows интеграциясын қолдау;
- * пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы;
- * өзіне-өзі қызмет көрсету порталы басқару агентін мобильді құрылғыға орнату, мобильді құрылғыларды қарау, құлыптау пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобильді құрылғысында деректерді жою мақсатында пайдаланушыларды қосу мүмкіндігін қамтамасыз етуі тиіс;
- * вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- * MicrosoftAzure және GoogleCloud бұлтты инфрақұрылымындағы қондырғылар;
- * openapi интеграциясы;
- * web консолін пайдаланып антивирустық қорғауды басқару;
- * әкімшілік консоліне рұқсатсыз кіру қаупін азайту үшін екі сатылы тексеру;
- * пайдаланушы тіркелгісінің параметрлерін өзгерткеннен кейін қосымша аутентификацияны қолданыңыз.
- * IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрау мүмкіндігі;
- * әкімшілік серверді қол жетімділігі жоғары жүйе ретінде орналастыру мүмкіндігі.
-
- Linux ОЖ негізіндегі орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қойылатын талаптар
- Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:
- o Debian GNU/Linux 11.x (Bullseye) 32 биттік / 64 биттік;
- o Debian GNU/Linux 10.x (Buster) 32 биттік / 64 биттік;
- o Debian GNU/Linux 9.x (Stretch) 32 биттік / 64 биттік;
- o Ubuntu Server 20.04 LTS (Focal Fossa) 64 бит;
- o Ubuntu Server 18.04 LTS (Bionic Beaver) 64 биттік;
- o CentOS 7.x 64 бит;
- o Red Hat Enterprise Linux Server 8.x 64 бит;
- o Red Hat Enterprise Linux Server 7.x 64 бит;
- O Suse LinuxEnterpriseServer 12 (барлық жаңарту бумалары) 64 бит;
- O Suse LinuxEnterpriseServer 15 (барлық жаңарту бумалары) 64 бит;
- o AstraLinuxSpecialEdition 1.7 (жабық бағдарламалық жасақтама режимі мен мандат режимін қосқанда) 64 бит;

- o AstraLinuxSpecialEdition 1.6 (жабық бағдарламалық жасақтама режимі мен мандат режимін қосқанда) 64 бит;
- o Astra Linux Common Edition 2.12 64 бит;
- О Альт Сервер 10 64 бит;
- О Альт сервері 9.2 64 бит;
- o Alt 8 SP сервері (LKNV.11100-01) 64 биттік;
- o Alt 8 SP сервері (LKNV.11100-02) 64 биттік;
- o Alt 8 SP сервері (LKNV.11100-03) 64 биттік;
- o OracleLinux 7 64 бит;
- o OracleLinux 8 64 бит;
- o red OS 7.3 64 биттік Сервер;
- o red OS 7.3 64 биттік сертификатталған басылым.
- Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек:
- o VMwarevSphere 6.7.
- o VMwarevSphere 7.0;
- o VMwareWorkstation 16 Pro;
- o Microsoft Hyper - V Server 2012 64 бит;
- o Microsoft Hyper - V Server 2012 R2 64 бит;
- o Microsoft Hyper - V Server 2016 64 бит;
- o Microsoft Hyper - V Server 2019 64 бит;
- o Microsoft Hyper - V Server 2022 64 бит;
- o CitrixXenServer 7.1 LTSR;
- o CitrixXenServer 8.x;
- o ParallelsDesktop 17;
- О ядроға негізделген Виртуалды машина. Келесі операциялық жүйелерді қолдайды:
- o Alt 8 SP сервері (LKNV.11100-01) 64 биттік;
- О Альт Сервер 10 64 бит;
- o AstraLinuxSpecialEdition 1.7 (жабық бағдарламалық жасақтама режимі мен мандат режимін қосқанда) 64 бит;
- o Debian GNU/Linux 11.x (Bullseye) 32 биттік / 64 биттік;
- o Ubuntu Server 20.04 LTS (Focal Fossa) 64 бит;
- o red OS 7.3 64 биттік Сервер;
- o red OS 7.3 64 биттік сертификатталған басылым
- Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі керек:
- o MySQL 5.7 Community 32 биттік / 64 биттік;
- o MySQL 8.0 32 биттік / 64 биттік;
- o MariaDB 10.5.x 32 бит / 64 бит;
- o MariaDB 10.4.x 32 бит / 64 бит;
- o MariaDB 10.3.22 және одан жоғары 32 биттік/64 биттік;
- o MariaDBServer 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік;
- o MariaDB 10.1.30 және одан жоғары 32 биттік/64 биттік.
- Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек:
- * орталықтандырылған антивирустық бағдарламалық жасақтаманы орнату, жаңарту және жою;
- * орталықтандырылған орнату, әкімшілік;
- * қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау;

- * саясат пен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;
- * қайта бөлу орын алатын триггерлердің иерархиялары;
- * жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
- * виртуалды машиналар желісін тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу;
- * әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігімен көп деңгейлі басқару жүйесін құру;
- * еркін деңгейдегі басқару серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
- * басқару серверлері үшін көп жалға алуды қолдау (multi-tenancy) ;
- * байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту;
- * басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қол жеткізу;
- * клиенттік компьютерлерге лицензияны автоматты түрде тарату;
- * орнатылған антивирустық қорғау Қосымшаларының жұмысында оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді баптау;
- * белгіленген бағдарламаларды лицензиялау деректері бойынша антивирустық қорғау оқиғалары бойынша графикалық есептерді құру;
- * жүйенің жұмысы туралы алдын ала конфигурацияланған стандартты есептердің болуы;
- * есептерді PDF және XML форматындағы файлдарға экспорттау;
- * антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин объектілерін орталықтандырылған басқару;
- * басқару серверінде аутентификация үшін ішкі есептік жазбаларды құру;
- * басқару жүйесінің кірістірілген құралдарын басқару жүйесінің сақтық көшірмесін жасау;
- * вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- * web консолін пайдаланып антивирустық қорғауды басқару;
- * басқару серверіне жүктемені азайту және кәсіпорын желісіндегі деректер трафигін оңтайландыру үшін басқару сервері арқылы да, тарату нүктелері арқылы да басқарылатын құрылғыларда антивирустық базалар мен бағдарламалық модульдерді жаңарту және тарату мүмкіндігі;

- • Жаңартуларды тексеру тапсырмасы арқылы жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын өнімділік пен қателерді тексеру мүмкіндігі;
- * антивирустық базалар мен бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары мүмкіндігін пайдалану мүмкіндігі.
-
- Антивирустық базаларды жаңартуға қойылатын талаптар
- Жаңартылатын антивирустық мәліметтер базасы келесі функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс:
- * күнтізбелік тәулік ішінде кемінде 24 рет антивирустық базаларды жаңарту ережелерін жасау;
- * жаңарту жолдарының көптігі, оның ішінде-байланыс арналары бойынша және иеліктен шығарылатын электрондық ақпарат тасымалдағыштарда;
- * электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру.
- Пайдалану құжаттамасына қойылатын талаптар
- Басқару құралдарын қоса алғанда, вирусқа қарсы қорғаудың барлық бағдарламалық өнімдері үшін пайдалану құжаттамасында Мемлекеттік стандарттардың талаптарына сәйкес орыс тілінде дайындалған құжаттар қамтылуға тиіс, оның ішінде:
- * "Пайдаланушы (әкімші) нұсқаулығы"
- Антивирустық құралдармен бірге жеткізілетін құжаттама тиісті антивирустық қорғаныс құралын орнату, конфигурациялау және пайдалану процесін егжей-тегжейлі сипаттауы керек.
- Техникалық қолдауға қойылатын талаптар
- Антивирустық бағдарламалық жасақтаманы техникалық қолдау:
- * Қазақстан Республикасының бүкіл аумағында антивирустық қорғау құралдарын өндірушінің және оның серіктестерінің сертификатталған мамандары электрондық пошта және Интернет арқылы орыс тілінде ұсынуға міндетті.
- * Антивирустық шешім өндірушісінің веб-сайты орыс тілінде болуы керек, антивирустық шешімді техникалық қолдауға арналған арнайы бөлім, толықтырылатын білім базасы, сондай-ақ бағдарламалық өнімдерді пайдаланушылар форумы болуы керек.

Келісті — Аманбаева М.Ж. (должность)