Конкурстық құжаттамаға сатып алынатын тауарлардың техникалық ерекшелігі

Сатып алудың нөмірі:	№ 17929599-1
Сатып алудың атауы:	46 пайдаланушыға арналған антивирустық қорғау лицензиясы.
Лоттың нөмірі:	№ 84299134-ЗЦП5
Лоттың атауы:	Бағдарламалық қамтамасыз ету
Лоттың сипаттауы:	бағдарламалық қамтамасыз етудің төлнұсқасы (тапсырыс бойынша бағдарламалық қамтамасыз етулерді әзірлеу бойынша қызметтерді қоспағанда)
Лоттың қысқаша сипаттауы:	Вирусқа қарсы бағдарлама 1 лицензия 46 қолданушыға (109)
Саны, көлемі:	1
Өлшем бірлігі:	Дана
Жеткізу орны:	751110000, Алматы қ., Алмалы ауданы Желтоқсан к-сі, 65
Жеткізу мерзімі:	келісімшартқа сайкес
Функционалдық, техникалық, сапалық және пайдалану мінездемесін сипаттау:	Сатып алудың мақсаты - қосымша ESET PROTECT Entry On Prem лицензияларын сатып алу арқылы қолданыстағы бағдарламалық жасақтама инфрақұрылымын кеңейту. Тұтынушының ағымдағы лицензиялау жүйесінің сипаттамаларымен толық үйлесімділікті қамтамасыз ету қажеттілігіне байланысты баламалы нұсқаларды жеткізуге рұқсат етілмейді. Әлеуетті өнім беруші 46 пайдаланушыға арналған ESET PROTECT Entry On Prem атаулы лицензиясын кемінде 12 күнтізбелік ай мерзімге ұсынуы тиіс. Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің «Әлеуметтік қорғау саласын дамытудың ұлттық ғылыми орталығы» ШЖҚ РМК атына рәсімделген, лицензия редакциясы және оның қолданылу мерзімі туралы деректер көрсетілген вирусқа қарсы бағдарламалық қамтамасыз ету өндірушісінің бірыңғай фирмалық лицензиялық келісімін ұсынуы тиіс. Өнім беруші жеңімпаз болып айқындалған және онымен мемлекеттік сатып алу туралы шарт жасалған жағдайда, лицензияланбаған бағдарламалық қамтамасыз етуді сатып алуға жол бермеу мақсатында өнім беруші Қазақстан Республикасының аумағында ESET компаниясының ресми серіктесі болуы тиіс. Оны растау үшін өнім беруші бағдарламалық қамтамасыз ету өндірушісінің авторизациялық хатын, сондай-ақ ESET серіктесінің сертификатын ұсынуы тиіс. Өнім беруші Тапсырыс берушіге өз өкілін жіберіп, антивирустық бағдарламаны компьютерлерге сол жерде қолмен орнатуға міндетті. Бұл ретте компьютерлердің бір бөлігі желіге қосылмаған. Басқару сервері 1. Бүкіл желілік инфрақұрылымның антивирустық қорғанысын орталықтандырылған басқару мүмкіндігі. 2. Бас серверден және бағынысты серверлерден тұратын әкімшілендірудің иерархиялық құрылымын құру мүмкіндігі. Бұл бас және өңірлік бөлімшелерге тиесілі жұмыс станцияларын, серверлерді және мобильді құрылғыларды антивирустық қорғауды орталықтандырылған басқаруды жүзеге асыруға мүмкіндік беруі тиіс. 3. Жекелеген клиентте қорғаныс модульдерін, оның ішінде жеке брандмауэрді, нақты уақыт режиміндегі қорғауды, пошта клиентін қорғауды, Интернетке қолжетімділікті қорғауды, құрылғыларды бақылауды, веббақылауды, спамға қарсы қорғауды қашықтан іске қосу және өшіру мүмкіндігі. 4. Қашықтан басқару құралы арқылы жұмысты аяқтау және қайта іске қосу, компьютерді ояту сигналын жіберу, хабарламалар жіберу, клиенттік компьютерде командалық жолдың нақты нұсқауларын орындау, клиенттік компьютердің операциялық жүйесін жаңартуды бастау сияқты қосымша желілік әрекеттерді орындау мүмкіндігі. 5. Соңғы нүктелердегі антивирустық өнімді қашықтан басқаруға, сондай-ақ жұмыс станцияларындағы антивирустық қорғау деңгейін және операциялық жүйенің жай-күйін бақылауға мүмкіндік беретін тәуелсіз агентті пайдалану. 6. Қашықтан әкімшілендіру құралының келесі дерекқорларды қолдауы: MS SQL Server, MySQL. 7. Үшінші тараптың HTTP-серверлері негізінде жаңартулар айнасын жасау мүмкіндігі. 8. Журналдар мен есептердің параметрлерін баптау немесе әртүрлі жүйелер/клиенттер үшін 50-ден астам үлгінің ішінен таңдау мүмкіндігі. 9. Жұмыс станциясында орнатылған бағдарламалық қамтамасыз етуді

бақылау, сондай-ақ таңдалған орнатылған бағдарламалық қамтамасыз етуді жою мүмкіндігі.
10. Физикалық немесе қашықтан қолжетімділік жоқ жұмыс станцияларында да антивирустық өнімдердің лицензиясын өшіру мүмкіндігі.
11. Тиісті лицензия бөлігімен алаң немесе филиал әкімшісін айқындау функционалының болуы.
12. Клондалған машиналарды қате сәйкестендіру туралы хабарлау үшін хабарламалар жүйесінде алдын ала орнатылған үлгілердің болуы. Бұл VDI жүйелерімен дұрыс бапталмаған интеграция туралы хабарлауға мүмкіндік беруі тиіс.
13. VDI жүйелерінде қай виртуалды машина көшіру немесе клондау үшін бастапқы көз болып табылатынын анықтау мүмкіндігі.
14. Компания филиалдарына сәйкес алаңдар құру функционалының болуы. Бұл лицензияның белгілі бір бөлігін жекелеген филиалдарға тағайындауға мүмкіндік беруі тиіс. Жұмыс станцияларын қорғау
1. Зиянды бағдарламалық жасақтамадан — компьютердегі файлдар кодының басына немесе соңына қосылатын белгілі бір зиянды кодтан қорғауды қамтамасыз ету. Зиянды бағдарламалық жасақтаманы анықтау машиналық оқыту компонентімен үйлесімдегі анықтау ядросы арқылы жүзеге асырылуы тиіс.
2. Вирустар немесе трояндар сияқты сөзсіз зиянды бағдарламаларға ұқсас түрде зиянды бағдарламалық жасақтамаға нақты жатқызуға болмайтын, алайда қосымша қажетсіз бағдарламалық жасақтаманы орнатуы, жүйе параметрлерін өзгертуі, сондай-ақ пайдаланушы күтпеген немесе растамаған әрекеттерді орындауы мүмкін ықтимал қалаусыз бағдарламалардан қорғауды қамтамасыз ету.
3. Интернет желісіндегі зиянкестерге жүйеге шектеусіз қолжетімділік беретін, сонымен бірге операциялық жүйеде өзінің бар екенін жасыратын қауіпті руткит бағдарламаларынан қорғауды қамтамасыз ету.
4. Зиянды болып табылмайтын, алайда оларды сканерлеу жұмыстың бұзылуына немесе жүйенің өнімділігіне әсер етуі мүмкін жекелеген файлдарды сканерлеуден алып тастау мүмкіндігі.
5. Нақты уақыт режимінде антивирустық қорғауды қамтамасыз ету.
6. Пайдаланушының немесе әкімшінің сұрауы бойынша және белгіленген кестеге сәйкес антивирустық сканерлеуді жүргізу.
7. Зиянды мінез-құлық пен зиянды бағдарламалық қамтамасыз етудің сипаттамаларын анықтау мақсатында кодты тереңірек талдау үшін машиналық оқыту технологияларын пайдалану мүмкіндігі.
8. Рұқсат етілген немесе тыйым салынған сыртқы құрылғылардың топтарын құру мүмкіндігі.
9. Браузерлерді қорғалған режимде іске қосуға мүмкіндік беретін қосымша модульдің болуы. Ол браузердің жад аймағына және оның терезелерінің мазмұнына араласу әрекеттерін бұғаттауды, сондай-ақ Интернет-төлемдер, Интернет-банкинг және т.б. сияқты маңызды Интернет-қосылымдарды қосымша қорғауды қамтамасыз етуі тиіс.
10. Жеке брандмауэрде оқыту режимінің болуы, бұл әкімшіге желілік қосымшалар мен жабдықтар үшін рұқсат беру қағидаларын қашықтан баптауға мүмкіндік береді.
11. Рұқсат етілмеген түрде дербес компьютердің белгісіз қауіпті желілерге қосылуын болдырмау мақсатында жеке брандмауэрде желіні қосымша аутентификациялау мүмкіндігі.
12. Желі бағдарламаларындағы жаңа рұқсат етілмеген желілік қосылымдарға әкелген өзгерістерді анықтай алатын жеке брандмауэрдің қосымша функционалының болуы.
13. Интернет желісіне қолжетімділігі жоқ жабық оқшауланған желілерде антивирустық қорғаудың өзектілігін сақтауға мүмкіндік беретін сервердегі жергілікті қоймадан клиенттердің жаңартуларын алу.
14. Тұрақты, тестілік және кейінге қалдырылған жаңартуларды алу режимінде жаңарту мүмкіндігі.
15. Барлық қолданыстағы желілік қосылымдар туралы толық ақпаратты көруге, сондай-ақ пайдаланушыға қорғалмаған Wi-Fi желісіне қосылу туралы ескертуге мүмкіндік беретін жеке брандмауэрдің қосымша функционалының болуы.
16. ДК-де бұғатталған IP-мекенжайлар тізімін көруге, олардың қара тізімге енгізілу себептері туралы ақпарат алуға және нақты қауіпсіз мекенжайларға ерекшелік жасауға мүмкіндік беретін жеке брандмауэрдің қосымша функционалының болуы.
17. Күдікті іске қосылған процестердің жұмысын бақылауға қабілетті жедел жадты сканерлеу модулі. Бұл мұқият шифрланған және жасырын қауіптердің өзінен жұқтыруды болдырмауға мүмкіндік беруі тиіс.
18. Операциялық жүйедегі рұқсат етілмеген және қауіпті өзгерістерді анықтау мақсатында операциялық жүйенің әртүрлі параметрлері мәндерінің маңыздылық деңгейін (қауіпті, белгісіз, аз белгілі, қауіпсіз) анықтау мүмкіндігі.
19. Скрипттерді құру және қашықтан орындау мүмкіндігі. Бұл қашықтағы

ДКде іске қосылған процестер мен қызметтерді тоқтатуға, тізілім тармақтарын жоюға, желілік қосылымдарды бұғаттауға мүмкіндік беруі тиіс.
20. Саясат арқылы тағайындалатын және редакциялау үшін қолжетімсіз антивирустық бағдарламалық қамтамасыз ету параметрлерін ДК-де уақытша өзгертуге жүйелік әкімшіге мүмкіндік беретін саясатты қайта анықтау режимінің болуы. Бұл антивирустық бағдарламалық қамтамасыз етуді нақты ортада икемді баптауды қамтамасыз етуі тиіс.
21. Қолданыстағы антивирустық өнімдердің ДК ресурстарын төмен деңгейде тұтынуы (барлық процестерді қоса алғанда: графикалық интерфейс, кешенді қорғау процесі, қашықтан әкімшілендіру қызметі): жедел жад — 50–100 МБ, орталық процессор — 2–35%.
22. Тұрақты, тестілік және кейінге қалдырылған жаңартуларды алу режимінде жаңарту мүмкіндігі.
23. Барлық пайдаланушылар немесе жекелеген пайдаланушылар/Windows немесе домен топтары үшін сыртқы құрылғыларды қосуға тыйым салу немесе рұқсат беру мүмкіндігі.
24. Сканерлеу үшін 64 биттік ядроны пайдалану, бұл жүйеге түсетін жүктемені азайтып, ең жылдам әрі тиімді сканерлеуді жүзеге асыруға мүмкіндік береді.
25. Компьютер белсенді емес күйде болған кезде сканерлеу мүмкіндігі.
26. Conficker, Sirefef, Necurs және басқа да күрделі тұрақты қауіптердің қалдықтарын тазартуға арналған бірнеше утилитаны біріктіретін кіріктірілген құралдың болуы.
27. Негізгі жүктеу жазбасында, соның ішінде UEFI интерфейсінде вирустардың бар-жоғын анықтау үшін жүктеу секторларын тексеру мүмкіндігі.
28. Қолдау көрсетілетін операциялық жүйелер: Microsoft Windows Vista (Professional немесе одан жоғары); Microsoft Windows 7 (Professional немесе одан жоғары); Microsoft Windows 8 (Professional немесе одан жоғары); Microsoft Windows 8.1 (Professional немесе одан жоғары); Microsoft Windows 10.
Серверлерді қорғау
1. Сервердің рөлдерін автоматты түрде анықтау және серверлік операциялық жүйенің жұмысына әсерді барынша азайтуға мүмкіндік беретін арнайы файлдарға, қалталарға, қосымшаларға арналған ерекшеліктерді автоматты түрде жасау.
2. UEFI интерфейсін сканерлеу — негізгі жүктеу жазбасында зиянды бағдарламалық қамтамасыз етудің бар-жоғын тексеру.
3. Компьютер белсенді емес күйде болған кезде сканерлеу.
4. Сканерлеу кезінде эвристикалық технологияларды пайдалану.
5. Зиянды бағдарламалардан, трояндық бағдарламалық қамтамасыз етуден, пернетақта шпиондарынан, жарнамалық бағдарламалардан, фишингтен, шпиондық бағдарламалық қамтамасыз етуден, руткиттерден, скрипттерден, ықтимал қалаусыз және қауіпті бағдарламалық қамтамасыз етуден қорғауды қамтамасыз ету.
6. Вирустық дерекқорларды тәулігіне кемінде 24 рет жоспарлы түрде жаңарту.
7. Негізгі серверден басқа резервтік әкімшілендіру серверлерін көрсету мүмкіндігі.
8. Құрылғы түрі, қолжетімділік деңгейі, өндірушісі, моделі немесе құрылғының сериялық нөмірі бойынша қолжетімділік қағидаларын құру арқылы жұмыс станциясына перифериялық құрылғылардың қосылуын бақылауды жүзеге асыратын құралдың болуы. Қағидалар барлық пайдаланушылар үшін де, жекелеген пайдаланушылар немесе Windows топтары үшін де құрылуы мүмкін.
9. Операциялық жүйенің жай-күйінің суреттерін жасауға мүмкіндік беретін жүйені диагностикалау құралының болуы. Бұл құрал операциялық жүйе жұмысының әртүрлі аспектілерін, оның ішінде іске қосылған процестерді, тізілім мазмұнын, орнатылған бағдарламалық қамтамасыз етуді және желілік қосылымдарды терең талдауға мүмкіндік беруі тиіс. Жүйенің әртүрлі жай-күй суреттерін салыстыру мүмкіндігінің арқасында бұл құрал жүйеде орын алған өзгерістерді анықтай алады. Сондай-ақ ол іске қосылған процестерді тоқтатуға, тізілім тармақтарын жоюға және желілік қосылымдарды бұғаттауға мүмкіндік беретін скрипттерді құрып, орындай алуы тиіс.
10. Интернеттен файлдарды көрсетілген кеңейтім бойынша жүктеуді бұғаттау мүмкіндігі.
11. Тұрақты, тестілік және кейінге қалдырылған жаңартуларды алу режимінде жаңарту мүмкіндігі.
12. Виртуалды жұмыс станцияларына, сондай-ақ жалпы гипервизорға түсетін жүктемені едәуір төмендететін арнайы технологияның болуы.
13. Терминал пайдаланушылары үшін графикалық интерфейсті өшіру арқылы іске қосу режимін баптау мүмкіндігі. Бұл терминал сервері режимінде жұмыс істейтін серверге түсетін жүктемені азайтуға мүмкіндік береді. Тауарды қабылдау және жеткізу тәртібі
1. Тапсырыс беруші тауарды жұмыс күндері жергілікті уақыт бойынша сағат 09:00-ден 16:00-ге дейін қабылдайды, егер Тараптар жазбаша түрде өзгеше

	келіспесе. 2. Жеткізуші тауарды жеткізудің болжамды күні мен уақытына дейін кемінде 24 (жиырма төрт) сағат бұрын Тапсырыс берушіні осы Шартта көрсетілген телефон нөмірі арқылы алдағы жеткізу туралы хабардар етуге міндетті. Хабарламада жеткізу күні, келудің болжамды уақыты, жеткізілетін тауардың атауы мен көлемі туралы ақпарат болуы тиіс. 3. Белгіленген мерзімде алдын ала хабарлама болмаған жағдайда, Тапсырыс беруші тауарды қабылдаудан бас тартуға немесе қабылдауды Тапсырыс берушіге қандай да бір айыппұл санкцияларын қолданбай, ең жақын мүмкін болатын күнге ауыстыруға құқылы. 4. Тауарды жеткізуді Тапсырыс берушіге тауарды беруге өкілеттігін растайтын құжаттары, сондай-ақ осы Шартта және қолданыстағы заңнамада көзделген барлық ілеспе құжаттары бар Жеткізушінің уәкілетті өкілі ғана жүзеге асырады. 5. Тауарды жеткізу Тапсырыс берушінің Шартта көрсетілген мекенжайдағы қоймасына дейін тауарды түсіруді Жеткізушінің күшімен және есебінен жүзеге асыруды қамтиды. Тауар Тапсырыс берушіге берілгенге және Тапсырыс берушінің қоймасында түсірілгенге дейін оның сақталуына Жеткізуші жауапты болады. 6. Жеткізушінің тауарды жеткізу жөніндегі міндеттемелері тауарды Тапсырыс берушінің қоймасына нақты жеткізгеннен, оны түсіргеннен, ілеспе құжаттарды бергеннен және Тараптардың уәкілетті өкілдері тауарға ілеспе құжаттарға (тауар жүккұжатына, қабылдау-тапсыру актісіне немесе Шартта көзделген өзге де құжатқа) қол қойғаннан кейін орындалды деп есептеледі.

Приложение 2
к конкурсной документации

Техническая спецификация закупаемых товаров к конкурсной документации

Номер закупки:	№ 17929599-1
Наименование закупки:	Антивирусная защита лицензия на 46 пользователей
Номер лота:	№ 84299134-ЗЦП5
Наименование лота:	Программное обеспечение
Описание лота:	оригинал программного обеспечения (кроме услуг по разработке программных обеспечении по заказу)
Дополнительное описание лота:	Антивирусная защита лицензия на 46 пользователей (109)
Количество:	1
Единица измерения:	Штука
Места поставки:	751110000, г.Алматы, Алмалинский район ул.Желтоксан, 65
Срок поставки:	согласно договора
Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров:	Требования к потенциальному поставщику. Предметом закупки является расширение существующей инфраструктуры программного обеспечения путем дозакупки дополнительных лицензий ESET PROTECT Entry On Prem. Поставка эквивалентов не допускается в связи с необходимостью обеспечения полной совместимости со спецификацией действующей лицензионной системы заказчика. Потенциальный поставщик должен предоставить именную лицензию ESET PROTECT Entry On Prem на срок не менее 12 календарных месяцев, на 46 пользователей. Предоставить единое фирменное лицензионное соглашение производителя антивирусного программного обеспечения, выписанное на РГГП "Национальный научный центр развития сферы социальной защиты" Министерства труда и социальной защиты населения Республики Казахстан с указанием данных о редакции и сроке действия лицензии. В случае определения его победителем и заключения с ним договора о государственных закупках, в целях недопущения приобретения нелицензионного программного обеспечения, поставщик должен являться официальным партнером компании ESET, на территории Республики Казахстан. В подтверждение этого поставщик должен предоставить авторизационное письмо от производителя программного обеспечения, сертификат партнера ESET. Поставщик обязан направить представителя к Заказчику и на месте вручную установить антивирус на компьютеры. При этом часть компьютеров не подключены к сети. Сервер управления 1. Возможность централизованного управления антивирусной защитой всей сетевой инфраструктуры. 2. Возможность построения иерархической структуры администрирования, которая состоит из главного сервера и подчиненных серверов, что дает возможность осуществлять централизованное управление антивирусной защитой рабочих станций, серверов и мобильных устройств, что принадлежат как главному, так и региональным подразделениям. 3. Возможность удаленно активировать и деактивировать модули защиты, такие как персональный брандмауэр, защита в режиме реального времени, защита почтового клиента, защита доступа в Интернет, контроль устройств, веб-контроль, антиспам на отдельно взятом клиенте. 4. Возможность выполнять с помощью инструмента удаленного управления дополнительные сетевые действия, такие как: завершение работы и перезагрузка, отправка сигнала пробуждения компьютера, отправка сообщений, выполнение конкретных инструкций командной строки на клиентском компьютере, старт обновления операционной системы клиентского компьютера. 5. Использование независимого агента, который позволяет осуществлять удаленное управление антивирусным продуктом на конечных точках, а также контролировать уровень антивирусной защиты на рабочих станциях и состояние операционной системы. 6. Поддержка инструментом удаленного администрирования следующих баз данных: MS SQL Server, MySQL. 7. Возможность создания зеркала обновлений на основе сторонних HTTPсерверов. 8. Возможность настраивать параметры журналов и отчетов или выбрать из более чем 50 шаблонов для различных систем/клиентов. 9. Возможность отслеживать установленное на рабочей станции ПО, а также удалять установленное ПО на выбор. 10. Возможность деактивировать лицензию антивирусных продуктов даже на

рабочих станциях, к которым нет физического или удаленного доступа.
11. Наличие функционала для определения администратора площадки или филиала с соответствующей частью лицензии.
12. Наличие предустановленных шаблонов в системе уведомлений для информирования о некорректной идентификации клонированных машин, что дает возможность оповещать о некорректно настроенной интеграции с системами VDI.
13. Возможность определять, какая виртуальная машина будет являться источником для копирования или клонирования в системах VDI.
14. Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам.
Защита рабочих станций
1. Предоставление защиты от вредоносного ПО – определенного вредоносного кода, который добавляется в начало или конец кода файлов на компьютере. Выявление вредоносного ПО должно осуществляться ядром обнаружения в сочетании с компонентом машинного обучения.
2. Предоставление защиты от потенциально нежелательных программ, которые нельзя однозначно отнести к вредоносному ПО по аналогии с такими безусловно вредоносными программами, как вирусы или трояны, но эти программы могут устанавливать дополнительное нежелательное ПО, менять настройки системы, а также выполнять неожиданные действия или действия, не подтвержденные пользователем.
3. Предоставление защиты от опасных программ руткитов, которые предоставляют злоумышленникам из Интернета неограниченный доступ к системе, в то же время скрывая свое присутствие в операционной системе.
4. Возможность делать исключения из сканирования определенных файлов, которые не вредоносные, но сканирование которых может привести к отклонениям в работе или влиять на продуктивность системы.
5. Обеспечение антивирусной защиты в режиме реального времени.
6. Антивирусное сканирование по требованию пользователя или администратора и в соответствии с графиком.
7. Возможность использования технологий машинного обучения для более углубленного анализа кода с целью выявления вредоносного поведения и характеристик вредоносного программного обеспечения.
8. Возможность создавать группы разрешенных или запрещенных внешних устройств.
9. Наличие дополнительного модуля, который позволяет запускать браузеры в защищенном режиме с целью блокирования попыток вмешательства в область памяти браузера и содержимого его окон, а также дополнительной защиты критических Интернет-соединений, таких как Интернет-платежи и Интернет-банкинг и т.д.
10. Наличие в персональном брандмауэре режима обучения, что позволяет администратору удаленно настраивать разрешительные правила для сетевых приложений и оборудования.
11. Возможность использовать в персональном брандмауэре дополнительную аутентификацию сети с целью предотвращения несанкционированного подключения ПК к неизвестным опасным сетям.
12. Наличие дополнительного функционала персонального брандмауэра, который способен обнаруживать те изменения в сетевых программах, которые повлекли за собой новые несанкционированные сетевые соединения.
13. Получение обновления клиентов из локального хранилища на сервере, что позволяет поддерживать актуальность антивирусной защиты в закрытых изолированных сетях, у которых нет доступа к сети Интернет.
14. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.
15. Наличие дополнительного функционала персонального брандмауэра, что позволяет просматривать всю подробную информацию по всем имеющимся сетевым соединениям, а также предупреждать пользователя о подключении к незащищенной сети Wi-Fi.
16. Наличие дополнительного функционала персонального брандмауэра, что дает возможность просматривать на ПК перечень заблокированных IPадресов, предоставляет информацию о причинах попадания в черный список и позволяет сделать исключения для конкретных безопасных адресов.
17. Модуль сканирования оперативной памяти, который способный отслеживать работу подозрительных запущенных процессов, что позволяет предотвратить заражение даже тщательно зашифрованными и скрытыми угрозами.
18. Возможность определения уровня критичности (опасный, неизвестный, малоизвестный, безопасный) значений различных параметров операционной системы с целью выявления несанкционированных и опасных изменений в операционной системе.
19. Возможность создавать и удаленно выполнять скрипты, что позволит на удаленном ПК останавливать запущенные процессы и службы, удалять ветки реестра, блокировать сетевые соединения.

20. Наличие режима переопределения политики, что дает системному администратору временную возможность изменять на ПК те настройки антивирусного ПО, которые назначаются политикой и недостижимые для редактирования, с целью гибкой настройки антивирусного ПО в специфической среде.
21. Низкое потребление ресурсов ПК актуальными антивирусными продуктами (совместно со всеми процессами: графический интерфейс, процесс комплексной защиты, служба удаленного администрирования): 50-100 МБ оперативной памяти, 2-35 % центрального процессора.
22. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.
23. Возможность запрещать или разрешать подключение внешних устройств как для всех, так и для отдельных пользователей или групп Windows или домена.
24. Использование 64-битного ядра для сканирования, что уменьшает нагрузку на систему и позволяет сделать самые быстрые и эффективные сканирования.
25. Сканирование компьютера в неактивном состоянии.
26. Наличие встроенного инструмента, что объединяет несколько утилит для очистки остатков сложных устойчивых угроз, таких как Conficker, Sirefef, Necurs и других
27. Возможность осуществлять проверку загрузочных секторов на наличие вирусов в главной загрузочной записи, в том числе интерфейса UEFI.
28. Поддержка ОС: Microsoft Windows Vista (Professional или выше); Microsoft Windows 7 (Professional или выше); Microsoft Windows 8 (Professional или выше); Microsoft Windows 8.1 (Professional или выше); Microsoft Windows 10.
Защита серверов
1. Автоматическое определение ролей сервера для создания автоматических исключений для специфических файлов, папок, приложений, позволяющее минимизировать влияние на работу серверной операционной системы.
2. Сканирование интерфейса UEFI – проверка на наличие вредоносного программного обеспечения в главной загрузочной записи.
3. Сканирование компьютера в неактивном состоянии.
4. Использование эвристических технологий во время сканирования.
5. Предоставление защиты от вредоносных программ, троянского ПО, клавиатурных шпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциального нежелательного и опасного ПО.
6. Регламентное обновление вирусных баз не менее 24 раз в сутки.
7. Возможность помимо основного указать резервные серверы администрирования.
8. Наличие инструмента, который сможет осуществлять контроль подключения к рабочей станции периферийных устройств путем создания правил доступа по типу устройства, по уровню доступа, по производителю, модели или серийному номеру устройства. Правила могут быть созданы как для всех, так и для отдельных пользователей или групп Windows.
9. Наличие инструмента для диагностики системы, который может создавать снимки состояния операционной системы для дальнейшего глубоко анализа различных аспектов работы операционной системы, включая запущенные процессы, контент реестра, установленное ПО, сетевые соединения. Благодаря умению сравнивать различные снимки состояния системы, этот инструмент может обнаружить изменения, которые произошли в системе. Также он может создавать и выполнять скрипты, что позволит останавливать запущенные процессы, удалять ветки реестра, блокировать сетевые соединения.
10. Возможность блокировать загрузку из Интернета файлов по указанному расширению.
11. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.
12. Наличие специальной технологии, значительно снижающей нагрузку на виртуальные рабочие станции, а также на гипервизор в целом.
13. Возможность настройки режима запуска путем отключения графического интерфейса для терминальных пользователей, что позволяет уменьшить нагрузку на сервер, работающий в режиме сервера терминалов.
Порядок приемки и поставки товара
1. Приемка товара Заказчиком осуществляется в рабочие дни с 09:00 до 16:00 часов по местному времени, если иное не согласовано Сторонами в письменной форме.
2. Поставщик обязан не позднее чем за 24 (двадцать четыре) часа до предполагаемой даты и времени поставки уведомить Заказчика о предстоящей поставке по номеру телефона, указанному в настоящем Договоре. Уведомление должно содержать информацию о дате, ориентировочном времени прибытия, наименовании и объеме поставляемого товара.
3. В случае отсутствия предварительного уведомления в установленный

	срок Заказчик вправе отказать в приемке товара либо перенести приемку на ближайшую возможную дату без применения к Заказчику каких-либо штрафных санкций. 4. Поставка товара осуществляется исключительно уполномоченным представителем Поставщика, имеющим при себе документы, подтверждающие полномочия на передачу товара, а также все сопроводительные документы, предусмотренные настоящим Договором и действующим законодательством. 5. Доставка товара включает его выгрузку силами и за счет Поставщика до склада Заказчика по адресу, указанному в Договоре. Поставщик несет ответственность за сохранность товара до момента его передачи Заказчику и завершения выгрузки на складе Заказчика. 6. Обязательства Поставщика по поставке считаются исполненными после фактической доставки товара на склад Заказчика, его выгрузки, передачи сопроводительных документов и подписания уполномоченными представителями Сторон товаросопроводительных документов (товарной накладной, акта приема-передачи либо иного документа, предусмотренного Договором).