Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасы Ішкі істер министрлігі Атырау облысының Полиция департаменті" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасы Ішкі істер министрлігі Атырау облысының Полиция департаменті" мемлекеттік мекемесі
Конкурстың №:	№ 17912320-1
Конкурстың атауы:	Лицензиялық бағдарламалық қамтамасыз етуді ұзарту жөніндегі қызметтері
Лоттың нөмірі:	№ 81448342-ОК1
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:	8973747.76
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	8973747.76
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	2026 жылдың 31 желтоқсанын қоса алғанда
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Техникалық ерекшелік Лицензиялық бағдарламалық қамтамасыз етуді (вирусқа қарсы бағдарлама) ұзарту жөніндегі қызметтері Жалпы талаптар Вирусқа қарсы қорғану (ВҚ) жұмыс станциялары мен серверлерінің жергілікті желісінде орнықты қызмет етуін қамтамасыз ететін, ауқымды шешімді ұсынуы қажет. Бүкіл ұйымның көлемінде бірыңғай вирусқа қарсы құралдар пайдаланылуы қажет. Жеке тұрған, яғни бірыңғай вирусқа қарсы қорғану жүйесіне қосылмаған, оның ішінде шалғай аумақта орналасқан дербес компьютерлер, өзіне залал келтіретін бағдарламалардың (антивирус) барлық түрлерінен қорғануды енгізетін, біріктірілген бағдарламалық өнімдермен қорғалған болуы тиіс. Басқару құралдарын қоса алғанда, барлық антивирустық құралдардың бағдарламалық интерфейсі орыс тілінде болуы тиіс. Барлық вирусқа қарсы құралдар, оған басқару құралдарын қосқанда, орыс тіліндегі мәнмәтіндік анықтамалық жүйесін иеленуі қажет. Шет елде кеңселері бар ұйымдар үшін АТ қызметкерлеріне арналған консоль мен серверді қайта орнатпай, әкімшілендіру серверіне қосылуға арналған басқару консолінің интерфейс тілін таңдау мүмкіндігі болуы тиіс. Барлық вирусқа қарсы құралдар, оған басқару құралдарын қосқанда, орыс тіліндегі мәнмәтіндік анықтамалық жүйесін иеленуі қажет. Вирусқа қарсы қорғанудың бағдарламалық құралдарының техникалық параметрлері келесі көрсетілген параметрлерге сәйкес келуі немесе үйлесуі қажет: Вирусқа қарсы құралдар мен орталықтандырылған басқару құралдарына енгізілуі қажет: • Вирусқа қарсы бағдарламалық қамсыздандыру (ВБҚ) пакеттеріне арналған кілттердің лицензияланған файлдары; бірнеше серверлермен сызбаларды пайдалану кезінде шалғай әкімгерлік кластерлік технология серверлар арасындағы байланыстарды ұйымдастыру үшін серверлар арасындағы байланысқа қосымша лицензиялар талап етілмейді. • жұмыс станцияларын, серверлерді және мобильдік құрылғыларын (смартфондар, планшеттер) вирусқа қарсы қорғанудың 700 қолданушыларға арналған ESET NOD32 бағдарламалық құралы; • пошталық серверлерді вирусқа қарсы қорғаудың бағдарламалық құралдары; • шлюздерді вирусқа қарсы қорғаудың бағдарламалық құралдары; • әкімгерлеу және қорғалатын тораптар сервері арасындағы байланысты орындау үшін әкімгерлеу агенті; • Windows, Linux/BSD ОС, Mac OS, мобилдік ОС Android орталықтанған басқаруы, мониторингі және жаңартудың бағдарламалық құралы; • орталықтандырылған басқарудың бағдарламалық құралдарының есептерді басқару және қалыптастыруға арналған WEB консолі болуы тиіс; • орталықтанған басқару кез келген құрылғыдан Web – браузер арқылы жүзеге асырылады; • орталықтанған басқарудың бағдарламалық құралы Windows және Linux платформаларына орнатылады; • деректердің вирусқа қарсы жаңартылған базасы және вирусқа қарсы ядроның компоненттері; • Прокси- сервер - жоғары ауқымдылықты шешімді қамтамасыз етуге және әкімгерлеудің орталық серверіне жүктемені төмендетуге арналған компонент; • Жергілікті желіде ДК автоматты іздеуді жүзеге асыратын, оларды қолмен іздеуді және қосуды жүзеге асыруды қажет етпей, белгісіз

	компьютерлерді табуға арналған құралдардың болуы; • Вирусқа қарсы бағдарламалық қамсыздандырудың клиенттік бөлігін әкімгерлеу агенттерін орнатудың келесі түрдегі әртүрлі нұсқаларының болуы: қашықтан немесе жергілікті: - Push орнату, - e-mail арқылы орнату, - жалғамалы тасушыны қолданумен, мәселен, USB орнату - Жергілікті орнату; • орыс тіліндегі пайдалану құжаттамасы. • Лицензияларды басқару үшін бөлінген бағдарламалық құралдардың болуы. Оның көмегімен лицензияларды, активацияланған модульдер және лицензиямен байланысты оқиғаларды, яғни әрекет ету, пайдалану және авторизациялау мерзімінің аяқталуын қадағалауға болады. • Орталықтанған басқару серверін пайдаланбай, вирусты сигнатураның жергілікті сақтау орнын құру үшін бөлінген құралдардыңк болуы. • Орталықтанған басқару серверінің консоль пайдаланушылардың қосфакторлы аутентификациясын ұйымдастыру мүмкіндігінің болуы. • кірістірілген құмсалғышты қоса алғанда өнімнің қауіпсіздігінің қосымша деңгейін қамтамасыз ету; Microsoft Windows түрлерінің ОЖ басқарылатын серверлерді вирустан қорғайтын бағдарламалық құралдарға қойылатын талаптар Microsoft Windows түрлерінің ОЖ басқарылатын серверлерді вирустан қорғайтын бағдарламалық құралдары ОЖ келесі нұсқаларында жұмыс істеуі қажет: • Microsoft Windows Vista; • Microsoft Windows Vista x64; • Microsoft Windows 7 • Microsoft Windows 7 x64. • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows 10 Microsoft Windows түрлерінің ОЖ басқарылатын файлды серверлерді вирустан қорғайтын бағдарламалық құралдар келесі функционалдық мүмкіндіктерді жүзеге асыруды қамтамасыз етуі қажет: • вирусқа қарсы бағдарламалық қамтамасыз ету интерфейсі сенсорлық экрандарды және жоғары рұқсат етілген экрандарды қолдауды қамтамасыз етуі қажет; • резидентті вирусқа қарсы мониторинг; • вирусқа қарсы БҚ интерфейсін толық жасыру мүмкіндігі; • пайдаланушының немесе әкімгердің командасы бойынша вирусқа қарсы сканерлеу; • кесте бойынша вирусқа қарсы сканерлеу; • белгілі-бір жағдайларда вирусқа қарсы сканерлеу: - деректердің вирусқа қарсы базасын жаңартудан кейін; - әрдайым компьютерді іске қосқан кезде; - әрбір тәулікте компьютерді бірінші қосқан кезде; - сәтті Ғаламторға немесе VPN қосу кезінде; - пайдаланушының кіруі; - күдікті белсенділікті, оның ішінде «нақты уақыт режимінде қорғау» белсенді модулін анықтаған кезде; - бос тұру күйі, компьютер бос тұрған жағдайда, келесі үш режимнің бірінде орналасқан жергілікті дискілерді автоматты түрде сканерлейді: басты бет, компьютерді құлыптау, пайдаланушының шығуы; • сканерлеу аяқталғаннан кейін ДК өшіру тапсырмасының болуы; • келесі протоколдар бойынша трафикті антивирустық сканерлеу: FTP, HTTP және HTTPs, POP3 және POP3s, сондай-ақ, трафик IMAP және IMAPs. • Microsoft Office құжаттарын қорғау және Internet Explorer арқылы өтетін файлдарды сканерлеу жөніндегі қосымша модульдің болуы; • эвристикалық талдау негізінде әлі белгісіз зиянды бағдарламалардан қорғау; • ДК-де олардың орналасуынан тәуелсіз

	тек белгілі қауіп-қатерлерді ғана қосу мүмкіндігі: • жасырын процестерді анықтау; • вирусқа қарсы қорғаудың қажетті компоненттерін ғана орнату мүмкіндігі (модульді орнату); • қажет болған жағдайда антивирустық қорғауды өшіру мүмкіндігі; • PKLITE, LZEXE, DIET, EXEPACK және т.б. типті бағдарламалармен қапталған файлдарды вирусқа қарсы тексеру және емдеу; • ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE формат мұрағатындағы файлдарды вирусқа қарсы тексеру және емдеу; • сыртқы әсер ету, өзгерту әрекеттерін болдырмау үшін, сондай-ақ реестр процестерін, файлдар мен кілттер мониторингі үшін Host Intrusion Prevention System (HIPS) болдырмаудың бапталған жүйесінің болуы; • сүзгілеудің алдын ала дайындалған режимімен бірге HIPS-те жұмыс істеу мүмкіндігі; • кез келген түрдегі есептеу желілерінде, соның ішінде сымсыз жүйелерді қоса алғанда, кіруді (IDS/HIPS) анықтау және болдырмау жүйесі бар желіаралық экранды пайдалану жолымен хакерлік шабуылдардан қорғауды қамтамасыз ету; • дербес файервол; • белгілі бір шарттарды орындау кезінде профильді автоматты түрде ауыстырумен бірнеше файервол профильдерін баптау мүмкіндігі; • екі бағытта компьютердің барлық желілік трафигін басқару; • трафикті төмен деңгейде сканерлеу; • IPv6 протоколын қолдау; • нөлдік күн қатерлерінен қорғау үшін кірістірілген құмсалғышты қолдау; • UEFI сканерлеу модулі; • шифрлау вирустарынан қорғаудың айрықша модулі; • кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден тапсырмаларды іске қосу; • бұғатталған немесе рұқсат етілген веб-сайттар тізімін құру арқылы, сондай-ақ, рұқсат етілген веб-сайттар тізіміне енгізілгендерден басқа барлық веб-сайттарға тыйым салу арқылы веб-ресурстарға қол жеткізуді басқару мүмкіндігі; • қосымшаларға арналған сүзгілеудің белсенді режимі, сондай-ақ, сүзгілеуді ажырату немесе айрықша қосымшаларға арналған пассивті режимге ауыстыру мүмкіндігі; • пайдаланушылар немесе пайдаланушылар топтары деңгейінде Ғаламтор желісін пайдалану саясатын қолдану ережелерін қоюға мүмкіндік беретін сайттар санаттары бойынша бапталатын веб-бақылау; • Веб-бақылау модулінде ескерту немесе блоктау бетін кастомизациялау мүмкіндігінің болуы • сенімді қосымшаларға арналған сүзу; • контекстік мәзірден сканерлеу; • сенім білдірілген веб-адрестерге арналған сүзгілеуді сөндіру; • сенімді IP адрестерді сүзуді сөндіру; • сенімді процестерді, сомалардың хэшін, файлдар мен папкаларды тексеруден алып тастау мүмкіндігі. • Ғаламтор желісінен жаңарту мүмкіндігі бар бірнеше жаңарту профильдерін (мысалы, мобильді пайдаланушылар үшін) баптау; • Жұмыс станциялары үшін вирусқа қарсы бағдарламалық қамтамасыз етуді (ВБҚ) әкімшілендіру агентінің болуы; • вирусқа қарсы БҚ клиентінде жоспарлаушының болуы; • ДК жағдайы туралы, орнатылған қосымшалар, қызметтер, желілік қосылулар және т.б. туралы жалпы ақпаратты өзгерістерді қадағалау және оларды автоматты түрде уақыт интервалы түсірілімі арқылы салыстыру мүмкіндігімен

	орталықтанған қарау мүмкіндігі, сондай-ақ, жүйенің қалпына келтіретін корректілі жұмысына өзгерту енгізу мүмкіндігі (процестер мен драйверлерді тоқтату, тізілім және жүйелік файлдар жазуларын жою және қалпына келтіру). • ядро және өнімнің барлық негізгі модулдері қайта жүктеуді қажет етпейді және орнатудан кейін бірден жұмыс істейді; • Вирусқа қарсы пакетпен мәселелерді шешудің жылдамдығын арттыру үшін вирусқа қарсы пакетті орнату және жұмыс істеуі туралы жүйелік конфигурация туралы журнал файлдарын жинауға арналған мамандандырылған утилитаның болуы; • бос тұрған күйде сканерлеу модулінің болуы, егер компьютер бос тұрған жағдайда, келесі үш режимнің бірінде орналасқан болса, автоматты түрде жергілікті дискілерді сканерлейді: тиегіш, компьютерді құлыптау, пайдаланушының шығуы; • әкімшілік ету агентін орнату арқылы қолданыстағы вирустық қарсы қорғану пакетін жою қажеттілігінсіз жұмыс станцияларын вирусқа қарсы қорғаудың орнатылған лицензияларын орталықтандырылған басқару серверіне қосу мүмкіндігі; • модемді біріктіру немесе VPN орнатудан кейін деректердің вирусқа қарсы базасын жаңартуды іске қосу; • белгілі-бір жағдайда немесе уақытша интервал бойынша вирусқа қарсы жоспарлаушыда бөгде өндірушінің қосымшасын іске қосу міндеттерін құру мүмкіндігі; • Web-парақшамен жүктелетін залал әкелуші сценарийлерден қорғау; • қажетсіз және жарнамалық хабарламаларды бұғаттау • өзін-өзі үйретететін антиспам; • пошта клиенттерін қорғау: Microsoft Outlook, Outlook Express,Windows Mail, Windows Live Mail; • антиспамның қара және ақ тізімдері, ерекшеліктер тізімі; • өткен тексеру уақытынан бері жағдайы өзгермеген объектілерді өткізу есебінен сканерлеу процесін жеделдету; • виртуализацияланған ортада сканерлеу жылдамдығын арттыруға арналған жалпы жергілікті кэшті пайдалану қызметінің болуы; • фишингтен қорғау: құпия сөз және басқаларды алу әрекетінен қорғайды; • құпия ақпараттарды, қалыпты веб-сайттар түрін қабылдайтын, залал келтіретін веб-сайттарға кіруге шектеу қою; • эксплойттардан қорғау: эксплойттерді бұғаттаушы процестердің өткізілуін бақылайды және нысаналы шабуылдар мен ертеде белгісіз эксплойттар – нөлдік күнгі қауіпке ұқсас болып келетін күдікті белсенділікті айқындайды; • процестердің әрекеттерін қадағалайтын жадыны сканерлеу модулінің және залал келтіретін процестер жадыда түрін өзгертуін алып тастаған кезде сканерлеудің болуы; • ботнеттен қорғау: зиянды бағдарламаларды олардың деректер алмасу сызбалары мен протоколдарын талдай отырып анықтауға көмектеседі; • тапсырмалардың бағдарлығына қарай вирусқа қарсы және басқа қосымшалар арасындағы жұмыс станциялары ресурстарын үлестіруді реттеу: вирусқа қарсы сканерлеуді фонды режимде жалғастыру мүмкіндігі; • параметрлер бойынша сканерлеу лимиттерін баптау - орналасу тереңдігі (мұрағаттар), объектінің өлшемі және объектіні сканерлеу уақыты; • деректерді сақтаудың қосылған сыртқы құрылғыларын автоматты түрде сканерлеу жүргізуге мүмкіндік беретін модулдің болуы, сондай-ақ, осындай құрылғылардан

	файлдарды іске қосу үшін кеңейтілген талдауды қолдану; • әрбір пайдаланушы үшін немесе пайдаланушылар тобына құрылғының типі бойынша (CD/DVD/Blu-Ray, USB деректер қоймасы, USB принтерлер, суреттерді өңдеу құрылғысы, FireWire құрылғысы, кард ридерлер, модемдер, LPT\COM порттар, Bluetooth құрылғысы) сонымен қоса берілген атрибуттар бойынша (пайдаланушы, модель, сериялық нөмірі) бірнеше құрылғы үшін бір ереже орнату кіруін шектеуді баптауға мүмкіндік беретін модулдің болуы; • MS NAP және CISCO NAC интеграциясы; • қосымша тоқтап қалған жағдайда, жадының апатты дамптарын құру мүмкіндігі • вирусты базаларды алдыңғы нұсқаға жаңартуды және көрсетілген аралық уақыт арқылы оларды кейін автоматты жаңартуды қосумен жаңартуды тоқтата тұру мүмкіндігі; • жаңарту кезінде вирус сигнатурасының және өнімдер модулінің деректер базасын үзілген жүктеулерді жаңарту қызметінің болуы; • Windows қауіпсіздік орталығымен интеграция; «міндетті емес» жаңартудан «сыниға» дейін жаңарту қажеттілігін таңдаумен, табылған үйлесімділіктерді жабатын патчтарды орнатуға арналған Windows жаңарту орталығымен интеграциялау; • жеке тапсырмалар ретінде компьютердің жүктелген аумағын және орындалатын файлдарды тексеруді баптау; • қосымша сервисімен қашықтан рұқсат етілмеген басқарудан қорғау, сондай-ақ залал келтіретін бағдарламалар, зиянкестер немесе біліксіз пайдаланушылар тарапынан қорғауды ажыратуды болдырмауға мүмкіндік беретін, құпиясөздердің көмегімен қосымша параметрлерге кіруді қорғау қосымшаларын өзі-өздігінен қорғау технологиясы; • жүйені өзекті жаңартудың болуын тексеру; • толық экранды режимде жұмыс істейтін қосымшаларға арналған вирустан қорғау жұмыстары кезіндегі хабарландыруларды автоматты түрде жасырудың бапталған қызметтерінің болуы, яғни толық экранды режимде қосымшаның жұміс істеуі кезінде вирусқа қарсы бағдарламалық қамтамасыз ету жұмысы туралы ақпараттық хабарлама экранда шықпайды; • әкімгерлерді жұмыс станцияларында болып жатқан маңызды оқиғалар туралы (пошталық хабарлама, қалқыған терезе, оқиғалар журналындағы жазба) хабарландырудың көп жолы болуы; • әртүрлі көздерден, байланыс каналдары арқылы және иеліктен шығарылған тасушы ақпараттардан вирусқа қарсы базаны және бағдарлама құралдарын жаңарту; • XML,TXT, DAT, DMP форматтарында логтар мен есептерді шығару; • белгісіз қауіпті детекирлеудің бұлтты технологиясының болуы, репутациялық сервистің негізінде қосымшаны бақылау; • залал келтіруші кодының үлгілерін автоматты немесе қолмен вирусты экспертке беру жүйесінің болуы; • апаттық қалпына келтіру дискілерін құру мүмкіндігі; • автономды қоректену режимінде электр энергиясын үнемдеу; • жүйелік талаптар аспауы тиіс: 300мб RAM, HDD 1гб, Processor Intel немесе AMD, бір ядролы, x86 немесе x64 1ГГц. • вирусқа қарсы пакеттің дистрибутива өлшемі 165 Мб аспауы қажет. Microsoft Windows түрлерінің ОЖ басқарылатын серверлерді вирустан қорғайтын бағдарламалық құралдарға қойылатын талаптар Microsoft Windows түрлерінің ОЖ басқарылатын

	серверлерді вирустан қорғайтын бағдарламалық құралдары ОЖ келесі нұсқаларында жұмыс істеуі қажет: • Microsoft Windows Server 2008 (x86 және x64) • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2008 x64 R2 SP1 / x64 R2 CORE • Microsoft Windows Server 2008 x86 SP2 / x64 SP2 CORE • Microsoft Windows Server 2012 x64 / x64 CORE • Microsoft Windows Server 2012 x64 R2 / x64 R2 CORE • Microsoft Windows Hyper-V Server 2008 R2 • Microsoft Windows Hyper-V Server 2012 • Microsoft Windows Hyper-V Server 2012 R2 Серверы Storage, Small Business және MultiPoint: • Microsoft Windows Storage Server 2008 R2 Essentials 1 жаңарту пакетімен • Microsoft Windows Storage Server 2012 • Microsoft Windows Storage Server 2012 R2 • Microsoft Windows Small Business Server 2008 (x64) • Microsoft Windows Small Business Server 2011 (x64) • Microsoft Windows Server 2012 Essentials • Microsoft Windows Server 2012 R2 Essentials • Microsoft Windows MultiPoint Server 2010 • Microsoft Windows MultiPoint Server 2011 • Microsoft Windows MultiPoint Server 2012 Microsoft Windows түрлерінің ОЖ басқарылатын файлды серверлерді вирустан қорғайтын бағдарламалық құралдар келесі функционалдық мүмкіндіктерді жүзеге асыруды қамтамасыз етуі қажет: • Вирусқа қарсы бағдарламалық қамтамасыз ету интерфейсі сенсорлық экрандарды және жоғары рұқсат етілген экрандарды қолдауды қамтамасыз етуі қажет; • Резиденттік вирусқа қарсы мониторинг; • пайдаланушының немесе әкімгердің командасы бойынша вирусқа қарсы сканерлеу; • кесте бойынша вирусқа қарсы сканерлеу; • белгілі-бір жағдайларда вирусқа қарсы сканерлеу: - деректердің вирусқа қарсы базасын жаңартудан кейін; - әрдайым компьютерді іске қосқан кезде; - әрбір тәулікте компьютерді бірінші қосқан кезде; - сәтті Ғаламторға немесе VPN қосу кезінде; - пайдаланушының кіруі; - күдікті белсенділікті, оның ішінде «нақты уақыт режимінде қорғау» белсенді модулін анықтаған кезде. • келесі протоколдар бойынша трафикті вирусқа қарсы сканерлеу: FTP, HTTP және HTTPs, POP3 және POP3s; • агентсіз негізде вирустың болуына Hyper-V вирусқа қарсы сканерлеу • эвристикалық талдау негізінде белгісіз зиян келтіретін бағдарламалардан қорғау; • сыртқы әсер ету, өзгерту әрекеттерін болдырмау үшін, сондай-ақ реестр процестерін, файлдар мен кілттер мониторингі үшін Host Intrusion Prevention System (HIPS) болдырмаудың бапталған жүйесінің болуы; • сүзгілеудің алдын ала дайындалған режимімен бірге HIPS-те жұмыс істеу мүмкіндігі; • тек белгілі-бір қауіптерді болдырмау үшін ДК-дің орналасқан орнына қарамастан қосу мүмкіндігі: • вирустың болуын тексеруге сканерлеу қосымшасының белгілі-бір процестерін шығарып тастау мүмкіндігі; • руткиттерді табу (жасырын файлдар/жүйелік аномалийлер); • PKLITE, LZEXE, DIET, EXEPACK және басқа типтегі бағдарламалар орнатылған файлдарды вирусқа қарсы тексеру және емдеу; • ARJ, BZ2, CAB, CHM, DBX, GZIP,

	ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE формат мұрағатындағы файлдарды вирусқа қарсы тексеру және емдеу; • тапсырмаларды кесте бойынша және/немесе операциялық жүйені жүктеуден кейін бірден іске қосу; • вирусқа қарсы жоспарлаушыда бөгде өндірушінің қосымшасын іске қосу міндеттерін құру мүмкіндігі; • Web-парақшамен жүктелетін залал әкелуші сценарийлерден қорғау; • команда жолы интерфейсінен вирусқа қарсы пакеттің параметрлерін баптау мүмкіндігі; • үздіксіз жұмыс істеу үшін сыни мәні бар, серверлердегі файлдарды автоматты түрде табу және алып тастау қызметі; • сканерлеу жылдамдығын арттыру үшін сканерлеу модулінің мөлшерін белгілеу мүмкіндігі; • бұғатталған не болмаса рұқсат берілген веб-сайттардың тізімін құру арқылы, сондай-ақ, бүкіл веб-сайттарғы шектеу қою арқылы, рұқсат етілгендер тізіміне енгізілгендерден басқа веб-ресурстарға кіруді басқару мүмкіндігі; • қосымшаларға арналған сүзгілеудің белсенді режимі, сондай-ақ, сүзгілеуді ажырату немесе айрықша қосымшаларға арналған пассивті режимге ауыстыру мүмкіндігі; • контекстік мәзірден сканерлеу; • сенім білдірілген веб-адрестерге арналған сүзгілеуді сөндіру; • көп ағынды сканерлеу; • жаңартудың бірнеше профилін ғаламтор желісінен жаңарту мүмкіншілігімен баптау (мәселен, мобильдік пайдаланушыларға арналған). • вирусқа қарсы пакетте жоспарлаушының болуы. • файлды серверлерге арналған вирусқа қарсы бағдарламалық қамтамасыз етуді (ВБҚ) әкімгерлеу агентінің болуы; • ДК жағдайы туралы, орнатылған қосымшалар, қызметтер, желілік қосылулар және т.б. туралы жалпы ақпаратты өзгерістерді қадағалау және оларды автоматты түрде уақыт интервалы түсірілімі арқылы салыстыру мүмкіндігімен орталықтанған қарау мүмкіндігі, сондай-ақ, жүйенің қалпына келтіретін корректілі жұмысына өзгерту енгізу мүмкіндігі (процестер мен драйверлерді тоқтату, тізілім және жүйелік файлдар жазуларын жою және қалпына келтіру); • ядро және өнімнің барлық негізгі модулдері қайта жүктеуді қажет етпейді және орнатудан кейін бірден жұмыс істейді; • әкімгерлеу агентін орнату арқылы, вирусқа қарсы қорғаудың қолда бар пакетін жоюды қажет етпей, орталықтанған басқару серверіне жұмыс станциясын вирустан қорғаудың орнатылған лицензиясын қосу мүмкіншілігі; • белгісіз қауіптен сақтанудың бұлтты технологиясы болуы, репутациялық сервис негізінде қосымшаларды бақылау; • модемді біріктіру немесе VPN орнатудан кейін вирусқа қарсы жаңартуды іске қосу; • өткен тексеру уақытынан бері өзгермеген жағдайдағы объектілерді өткізу есебімен сканерлеу процесін жылдамдату; • вирусқа қарсы пакетпен туындауы мүмкін мәселелер кезінде мәселелерді шешуді жылдамдату үшін вирусқа қарсы пакетін орнату және жұмыс істеуі, жүйесі конфигурациясы туралы журнал файлдарын жинауға арналған арнайыландырылған жабдықтардың болуы; • виртуализацияланған ортада сканерлеу жылдамдығын арттыруға арналған жалпы жергілікті кэшті пайдалану қызметінің болуы; • фишингтен қорғау: құпия сөз және басқаларды алу әрекетінен қорғайды; құпия ақпараттарды,

	қалыпты веб-сайттар түрін қабылдайтын, залал келтіретін веб-сайттарға кіруге шектеу қою; • эксплойттардан қорғау: эксплойттерді бұғаттаушы процестердің өткізілуін бақылайды және нысаналы шабуылдар мен ертеде белгісіз эксплойттар – нөлдік күнгі қауіпке ұқсас болып келетін күдікті белсенділікті айқындайды • нөлдік күн қатерлерінен қорғау үшін кірістірілген құмсалғышты қолдау; • UEFI сканерлеу модулі; • шифрлау вирустарынан қорғаудың айрықша модулі; • желілік шабуылдардан қорғау модулі; • ботнеттен қорғау модулі; • жады сканерлеу модулінің бар болуы, ол процестер мінез-құлқын қадағалайды және олар жадында бүркемеленуді алып тастағанда зиянды процестерді сканерлейді; • міндеттердің басымдығына байланысты вирусқа қарсы қорғану пен басқа қосымшалар арасында сервер ресурстарын бөлуді реттеу: фондық режимде вирусқа қарсы сканерлеуді жалғастыру мүмкіндігі; • Параметрлер бойынша сканерлеу шектерін орнату - ұяшықтың тереңдігі (мұрағаттар), нысан өлшемі және нысанды қарап шығу уақыты; • ауысымды ақпарат тасығыштарды және құрылғыларды бұғаттау (USB); • әрбір пайдаланушы үшін немесе пайдаланушылар тобына құрылғының типі бойынша (CD/DVD/Blu-Ray, USB деректер қоймасы, USB принтерлер, суреттерді өңдеу құрылғысы, FireWire құрылғысы, кард ридерлер, модемдер, LPT\COM порттар, Bluetooth құрылғысы) сонымен қоса берілген атрибуттар бойынша (пайдаланушы, модель, сериялық нөмірі) бірнеше құрылғы үшін бір ереже орнату кіруін шектеуді (рұқсат жоқ/тек оқуға/толық рұқсат берілді/ескерту) баптауға мүмкіндік беретін модулдің болуы; • Windows қауіпсіздік орталығымен интеграциялау; • «міндетті емес» жаңартудан «сыниға» дейін жаңарту қажеттілігін таңдаумен, табылған үйлесімділіктерді жабатын патчтарды орнатуға арналған Windows жаңарту орталығымен интеграциялау; • Windows Management Instrumentation қолдау • жеке тапсырмалар ретінде компьютердің жүктелген аумағын және орындалатын файлдарды тексеруді баптау; • Вирусқа қарсы БҚ автоматты біріктіру мүмкіндігімен кластерлі жүйені қолдау (кластердегі БҚ конфигурациясын автоматты синхрондау) • қосымша сервисімен қашықтан рұқсат етілмеген басқарудан қорғау, сондай-ақ, залал келтіретін бағдарламалар, зиянкестер немесе біліксіз пайдаланушылар тарапынан қорғауды ажыратуды болдырмауға мүмкіндік беретін, құпиясөздердің көмегімен қосымша параметрлерге кіруді қорғау қосымшаларын өзі-өздігінен қорғау технологиясы; • операциялық жүйенің өзекті жаңартуларын тексеру; • команда жолы арқылы ВБҚ графикалық интерфейссіз, әкімгерлеу және конфигурациялаусыз жан-жақты жұмыс істеу; • ВБҚ конфиграциялауға және қандай да бір әрекеттерді орындауға мүмкіндік беретін сценарийлерді орындау есебінен жұмыстарды автоматтандыру мүмкіндігі; • толық экран режимінде вирусқа қарсы жұмыс істеу кезінде хабарламаны автоматты жасыру; • толық экран режимінде жұмыс істейтін қосымшаларға арналған вирусқа қарсы жұмыстар кезіндегі хабарламаларды автоматты жасырудың бапталатын функцияларының болуы; • әкімгерлерді жұмыс станцияларында болып жатқан

	маңызды оқиғалар туралы (пошталық хабарлама, қалқыған терезе, оқиғалар журналындағы жазба) хабарландырудың көп жолы болуы; • әртүрлі көздерден, байланыс каналдары арқылы және иеліктен шығарылған тасушы ақпараттардан вирусқа қарсы базаны және бағдарлама құралдарын жаңарту; • залал келтіруші кодының үлгілерін автоматты немесе қолмен вирусты экспертке беру жүйесінің болуы; • апаттық қалпына келтіру дискілерін құру мүмкіндігі; • вирусқа қарсы пакеттің дистрибутива өлшемі 127 Мб аспауы қажет. Мобильдік құрылғыларды вирустан қорғау құралдарына қойылатын талаптар: Смартфондарды вирустан қорғаудың бағдарламалық құралдары келісі қызметтерді қамтамасыз етуі қажет: • Құрылғы қауіпсіздігі аудитін есепті түрлендіре отырып жүргізу мүмкіндігі; • Смартфондар мен планшеттердің файлды жүйесін үнемі қорғау; • Барлық қосымшаларды, файлдарды, папкалар мен жады карталарын нақты уақыт режимінде тексеру; • Смартфонда немесе жадыны ұлғайтудың қосылған карталарында тұрған файлдар жүйесінің объектілерін пайдаланушының талабы немесе кесте бойынша тексеру; • Зиян келтірілген объектілерді карантинді сақтау орнында сенімді оқшаулау; • Зиян келтіретін бағдарламаларды іздеу және қауіпті объектілерді жою кезінде пайдаланылатын вирусқа қарсы базаны жаңарту; • Қалаусыз SMS және MMS хабарламаларды бұғаттау; • Орнатылған қосымшаларды бақылауға, белгілі-бір қосымшаларға кіруді бұғаттауға және пайдаланушыға кейбір бағдарламаларды жоюды ұсынумен, қауіп дәрежесін төмендетуге арналған қосымшаларды қадағалау; • Минималды қауіпсіздік деңгейінің тапсырмасы және экранды бұғаттан шығару кодының қиындығы; • Бұғаттан шығарудың сәтсіз әрекеттерінің минималды мөлшерін көрсету; • Экранды бұғаттан шығаруға арналған әрекеттің максималды мерзімін көрсету; • Экранды бұғаттау таймеріне баптау; • Камераны пайдалануды шектеу; • фишингтен қорғау: құпия сөз, банк деректемелері мен өзге құпия ақпараттарды өздерін заңды деп көрсететін заңсыз веб-сайттармен алу әрекетінен қорғайды. • Хабарландыру орталығы: әртүрлі оқиғалар туралы, олардың корпоратвитік саясатқа сәйкессіздік себептері және осы үйлесімсіздікті жою туралы мәліметтер беру; • Смартфонды ұрлаудан және жоғалтудан қорғау. Мобильдік құрылғыны қашықтан бұғаттау мүмкіндігін қамтамасыз ету; • Смартфоннан ақпараттарды қашықтықтан жою мүмкіндігі; • Сенім білдірілген SIM-картаны анықтау мүмкіндігі; • SMS-хабарлама арқылы сенімсіз SIM-картаны пайдалану туралы ескертумен, хабарландыруды автоматты жасырын жөнелту. Сонымен қатар, хабарлама зиянкестерді сәйкестендіру үшін қажетті ақпараттарды енгізуі қажет: ағымдағы SIM-картаның телефон нөмірі, телефонның IMSI нөмірі және IMEI нөмірі; • Зауыттық қондырғыларға дейін ұлғайтылған алып тастау: құрылғыда барлық қолжетімді деректер жойылады (файлдардың тақырыпаттары жойылады). Сонымен қатар, телефонда зауыттық баптаулар әдепкі қалпы бойынша қалпына келтіріледі. • Дабылды қосу мүмкіндігі: Жоғалған құрылғы бұғатталады және тіпті егер құрылғының дауысы сөндірулі

	болса да өте қатты дауыс бере бастайды; • Вирусқа қарсы бағдарламалық қамтамасыз етуді (ВБҚ) әкімгерлеудің кіріктірілген агентінің болуы; Вирусқа қарсы қорғауды басқару жүйесіне талаптар Барлық қорғалатын ресурстар үшін басқарудың бағдарламалық құралдары келесідей мүмкіндіктердің іске асырылуын қамтамасз етуі керек: • Ауқымды шешімдер: ауқымды сервермен пайдалану есебімен жүргізіледі • Бағдарламалық вирусқа қарсы интерфейс сенсорлы экрандардың және жоғары ауқымды экрандарды қолдауды қамтамасыз етуі керек; • Прокси-сервер – әкімшілік орталық серверіне жүктемесін шешу және төмендету жоғары масштабтауды қамтамасыз ету үшін • Белгісіз компьютерлерді анықтау үшін аспаптардың болуы, локалды жүйенің ДК автоматты іздеуді, оларды қолмен іздеуді және қосуды жүзеге асыруды қажет етпей жүзеге асыру; • вирусқа қарсы қорғаудың бағдарламалық құралдарын орталықтандырылған орнату/жаңарту/жою, баптау, әкімшілендіру; • ақпаратты орталықтандырылған жинау және вирусқа қарсы қорғаудың жай-күйі туралы есептер жасау; • сервер мен клиент арасындағы қорғалған байланыс; • Орталықтандырылған басқарудың бағдарламалық құралдары есептерді құру және басқару үшін WEB консоль болуы керек; • Орталықтандырылған басқару кез келген Web - браузер арқылы жүзеге асырылуы мүмкін; • Графикалық түрде есеп жасау; • HTML,TXT, CSV, PDF форматтарында лот пен есептердің экспорты; • SIEM қолдау модулінің болуы; • Клиенттер мен группаларға арналған алдын ала бағдарлама (жаңарту түрлері, қолдануға тыйым салынған сайттар, жоспарлаушының кестесі және т.б.); • хабарлама жіберу мүмкіндіктері, мобильді құрылғыға жіберу сияқты, сондай- ақ жеке компьютерлерге сияқты; • мобильді құрылғыдан қауіпсіздік аудит журналын қашықтан жасау мүмкіндігі; • пайдаланушы қосымшаларын орнату мүмкіндігі; • вирусқа қарсы бағдарламалық қамтамасыз етудің клиенттік бөлігін басқару агенттерін орнатудың әртүрлі нұсқаларының болуы: қашықтан немесе жергілікті: - Push орнату, - e-mail арқылы орнату, - USB сияқты алмалы-салмалы тасымалдаушыны орнату, - Жергілікті орнату; • операциялық жүйелерге арналған агенттің тиісті орнату пакетін немесе қолмен басқару режимінде автоматты таңдау мүмкіндігінің болуы. • клиенттер үшін қауіпсіз саясатты баптау; • ДК жағдайы туралы, орнатылған қосымшалар, қызметтер, желілік қосылулар және т.б. туралы жалпы ақпаратты өзгерістерді қадағалау және оларды автоматты түрде уақыт интервалы түсірілімі арқылы салыстыру мүмкіндігімен орталықтанған қарау мүмкіндігі, сондай-ақ, жүйенің қалпына келтіретін корректілі жұмысына өзгерту енгізу мүмкіндігі (процестер мен драйверлерді тоқтату, тізілім және жүйелік файлдар жазуларын жою және қалпына келтіру); • жүйенің сыни объектілерін жоюға/өзгертуге арналған ақырғы клиенттерге белгілі-бір сценарийді қашықтан қосу мүмкіндігі. • вирустан қорғауды басқару жүйесін орнатудан кейін ДК қайта жүктеу қажеттілігінің болмауы; • вирустан қорғау және вирусқа қарсы базаның бағдарламалық құралын автоматты жаңарту; • жеке компьютерлер немесе топтарға

	арналған сигнатуралық базаларды жаңартуды жылдам жіберуді жүргізу мүмкіндігі; • оларды алған соң бірден пайдаланушының жұмыс орнына жаңартуды жеткізу; • орталықтанған карантин; • Active Directory құрылымы негізінде қолмен және автоматты басқарылатын компьютер тобын құру мүмкіндігі; • Active Directory-мен кесте бойынша және қолмен синхронизациялау мүмкіндігі; • желі топологиясын есепке алумен қорғалмаған жұмыс станцияларын автоматты іздеу; • есептік жазулар бойынша серверлерді баптаудағы өзгерту аудиті; • әкімгерлер мен операторлар рөлін, сондай-ақ, әрбір деңгейде ұсынылатын есептеме түрлерін баптау мүмкіндігімен басқарудың көп деңгейлі жүйесін құру; • әртүрлі көздерден, байланыс каналдары мен ақпараттар тасушыларды бағдарламалық құралдарды және вирустан қорғау базасын жаңарту; • вирустан қорғаудың орнатылған қосымшаларсындағы жұмыстарда болған оқиғалар туралы хабарлау механизмі және олар туралы пошталық хабарламаны үлестіруді баптау мүмкіндігі; • залал келтіруші кодының үлгілерін автоматты немесе қолмен вирусты экспертке беру жүйесінің болуы; • динамикалық топты құру мүмкіндігі, ол аталған топтардың шарттарына сәйкес клиникалық станцияларды динамикалық тұрғыда қосады; • статикалық және динамикалық топтармен жұмыс істеу; • желінің әкімгерін хабарландырудың әртүрлі нұсқасы (e-mail, SNMP-қақпанды пайдалану); • деректер базасының ішіндегіні резервтік көшірмесін құру және серверді баптау мүмкіндігі; • пайдаланушының доменді атын және құпиясөзді пайдаланумен қашықтан әкімгерлеу серверінің консоліне қосылу мүмкіндігі; • серверлерді және Windows, Linux\BSD жұмыс станцияларын, сондай-ақ, мрбильдік ОЖ (Android) қорғауға арналған шешімдерді әкімгерлеу; • Wake on LAN локалді желісі бойынша ояту функциясының болуы; • жабдықтың іздерін анықтаудың күрделі логикасы арқылы «клондалған машиналарды» автоматты анықтау мүмкіндігі. • "PNS" (Push Notification Service) және WOL үшін көп адресті шақыруларды қолдаумен репликация үшін протоколының болуы. • жабдықтарды түгендеуге арналған функционал. • әкімшілік серверімен деректер алмасуды тоқтату немесе жалғастыру үшін таңдалған компьютерлерде ескертулерді жылдам ажырату немесе қосу функциясының болуы; • MS SQL, MySQL деректер базасын қолдау; • Орталықтанған басқарудың бағдарламалық құралдары Windows және Linux платформаларында орнатыла алады • Бағдарламалық құралдар Windows және Linux платформаларының бас тартуға тұрақты кластеріне орнатылуды қолдауы қажет • Қашықтан әкімгерлеу серверінде мына опеарциялық жүйелер орнатылуы және қолдауы қажет Windows Server: o Windows Server 2003 x86 SP2 /x64 SP2 o Windows Server 2003 x86 R2 SP2 /x64 R2 SP2 o Windows Server 2008 x64 R2 SP1 / x64 R2 CORE o Windows Server 2008 x86 SP2 / x64 SP2 o Windows Server 2012 x64 / x64 CORE o Windows Server 2012 x64 R2 / x64 R2 CORE o Microsoft SBS 2003 x86 SP2 / x86 R2 o Microsoft SBS 2008 x64 SP2 o Microsoft SBS 2011 x64 Standard / x64 Essential Linux: o Ubuntu 12.04 LTS x86 Desktop / Server o Ubuntu 12.04 LTS

	x64 Desktop / Server o Ubuntu14.04. LTS x86 Desktop / Server o Ubuntu 14.04 LTS x64 Desktop / Server o RHEL Server 6 x86 / x64 o RHEL Server 7 x86 / x64 o CentOS 6 x86 / x64 o CentOS 7 x86 / x64 o SLED 11 x86 / x64 o SLES 11 x86 /x64 o OpenSUSE 13 x86 / x64 o Debian 7 x86 / x64 o Fedora 19 x86 / x64 • Орталықтан басқару, мониторинг және жаңартудың бағдарламалық құралдары келесі нұсқалардың виртуалды платформаларында жұмыс істеуі қажет: o VMware vSphere/ESXi (5.0 нұсқасы және жаңасы) o VMware Workstation (9 нұсқасы және жаңасы) o VMware Player (7 нұсқасы және жаңасы) o Microsoft Hyper-V (Server 2012 және 2012 R2) o Oracle VirtualBox (4.3.24 нұсқасы және жаңасы) Лицензиялармен басқаруға арналған бөлінген бағдарламалық аспаптардың болуы. Оның көмегімен лицензияларды, активтендірілген модулдерді және лициензиямен байланысты әрекет ету, пайдалану және авторизациялау мерзімдерінің аяқталуы секілді оқиғаларды қадағалауға болады. Құралдармен әртүрлі рөлдерде лицензия иесі немесе қауіпсіздік әкімгері сияқты жұмыс істеу. Келесі әрекеттерді орындау мүмкіндігі: • Нақты уақыттағы лициензия жағдайын көріп отыру; • Жеке құрылғыларды бақылау (бұл ретте оларды ажырату); • Лицензия оқиғаларымен байланысты хабарламаны баптау; • Лициензияларды ескі және жаңа нысанда біруақытта аралас ортада сақтау; • Бағдарламаны активациялауға болатын, электрондық пошта және құпия сөздер хабарламасына лицензия кілтін алмастыру; • Бір есептік жазбаға бірнеше лицензия белгілеу; • Басқа адамдарға лицензияны пайдалануға (оларды активациялауға) рұқсат беру; • Лицензия жағдайын біршама қолайлы бақылауға арналған хабарламаны баптау; • Орталықтанған басқару серверімен синхрондау функциясының болуы; • Оқиғалар журналының ақпараттық базасын және саясатын баптауды сақтаумен, вирусқа қарсы бағдарламалық қамтамасыз ету дің біршама ертедегі нұсқаларын дұрыстау үшін бөлінген аспаптардың болуы. • Орталықтанған басқару серверін пайдаланбай, вирусты сигнатураны локалды сақтау орнын құру үшін бөлінген аспаптардың болуы. • Орталықтан басқару сервері консолін пайдаланушыларды екі факторлы аутентификациялауды ұйымдастыру мүмкіндігінің болуы. Орталықтан басқару сервері консолін 10 пайдаланушыға арналған екі факторлы аутентификациялауды қолдау. Аталған қызметті пайдалану кезінде дәл сондай өндірушінің екі факторлы аутентификация шешімі және вирусқа қасры бағдарламалық қамтамасыз етудің пакеті пайдаланылуы қажет. • басқару серверінде тапсырма құру арқылы тораптарда лицензияларды деактивациялау мүмкіндігінің болуы. Жаңа, бұрын белгісіз қауіп-қатерлерді анықтау үшін машиналық оқыту технологиялары негізінде орнатылған құмсалғыш көмегімен жұмыс станцияларын, файлдық және пошта серверлерін қорғауға арналған өнімдердің қосымша қауіпсіздік деңгейі сервисі. Сервисте келесі функционалдылық іске асырылуы тиіс: • Мінез-құлықты талдау негізінде детектрлеу • Машиналы оқыту • Нөлдік күннің қауіптерін анықтау • Кірістірілген құмсалғыш Жаңа, бұрын белгісіз қатерлерді анықтау үшін

	машиналық оқыту технологиясы негізіндегі сервис жұмыс станцияларын, тапсырыс берушінің жергілікті желісінің файлдық серверлерін антивирустық қорғау бойынша шешім құрамында жеткізіледі. • Жеке лицензиямен белсендірілетін қосымша функционалдықты вирусқа қарсы өнімдермен қолдауының болуы. Сервис сервистің өзі сияқты вирусқа қарсы қамтамасыз ету өндірушісінің өнімдеріне арналған. Сервис жүйенің қауіпсіздігін қамтамасыз ету орталығынан іске қосылуы және басқарылуы тиіс. • Сервис жұмыс станцияларын, файлдық серверлер мен пошта серверлерін қорғау бойынша вирусқа қарсы шешімдермен жұмысты қолдауы тиіс. • Сервистермен жұмыс істеу үшін тек интернет желісіне кіру қажет, тапсырыс берушінің желісінде ешқандай аппараттық құралдар қажет емес. Сервис қамтамасыз етуі тиіс: • Көп деңгейлі қорғауды - машинамен оқытудың кемінде 3 моделі болуы тиіс. Жүйе виртуалды ортада немесе құмсалғышта үлгілермен жұмыс істейді. Жүйе зиянды бағдарламалардың үлгілерін алдау үшін пайдаланушылардың мінез-құлқын модельдейді және зиянды бағдарламалардың барлық белгілі үлгілерінің мінез-құлқымен үлгілердің мінез-құлқын салыстыру үшін Deep Learning нейрондық желілерінің модельдерін пайдаланады. • Нақты шолу - Әрбір зерттелетін үлгі қауіпсіздік орталығының консолінде бейнеленеді, онда оның сипаттамалары мен шығу тегі туралы егжей-тегжейлі ақпарат көрнекі және ыңғайлы болады. • Талдаудың жоғары жылдамдығы - 5 минут ішінде белгісіз үлгілердің 90% талдауын ұсыну • Мобилділік – корпоративтік желіде немесе одан тыс жерде пайдаланушылардың орналасқан жеріне қарамастан файлдарды талдау мүмкіндігінің болуы. • Күдікті файлдарды қолмен немесе автоматты түрде саясат конфигурациясы негізінде жіберу мүмкіндігі болуы. • Файлдарды Қауіпсіздікті қамтамасыз ету орталығының веб-консолінен немесе белсендірілген сервисі бар клиенттік компьютерлерден қолмен жіберу мүмкіндігі. • Қауіпсіздікті қамтамасыз ету орталығының API арқылы сервис әрекеттерін басқару мүмкіндігі • 64 Мб дейін көлемді үлкен файлдарды жіберу мүмкіндігі болуы; • Тексеруге жіберу үшін қолдау көрсетілетін файл түрлері: • Мұрағаттар (.zip,. rar, .7z, .bzip2 және басқалар) – пошта серверлерін қорғау өнімдерін пайдаланғанда • Құжаттар (.docx, .xslx, .rtf және басқалар) • Орындалатын файлдар (.exe, .dll, .sys және басқа файлдар) • JAR, LNK, REG, MSI, SWF және басқалар • Сценарийлер (.bat, .cmd, .js, .vbs, .ps және басқалар) • Ole2 - пошта серверлерін қорғау өнімдерін пайдаланған кезде; • .hta • Пошта серверлерін қорғау жөніндегі өнімдермен пайдалану кезінде – құмсалғышта талдау кезінде шифрланған архивтер үшін парольдерді іріктеу функционалының болуы; • Бақыланатын үлгінің мінез-құлқының қысқаша сипаттамасы келтірілетін тексерілген үлгінің мінез-құлқы туралы есеп беру функционалдығының болуы. Файл туралы есепте келесі ақпарат болуы керек: • Файлды жіберген компьютердің аты; • файлды жіберген бастапқы компьютерде пайдаланушыны көрсету. Кейбір жағдайларда бұл жүйелік пайдаланушы болуы мүмкін. • Жіберу себебі (автоматты түрде, қолмен). • файлды

	алған бұлттың бөлігі көрсетілген; • Хеш SHA1 жіберілген файл. • Файл атауы және оның жіберушілердің файлдық жүйесіндегі толық жолы. • Файлдың көлемі. • Файл санаты (файл түрі). • Есепте параметрлердің болуы: Жағдайы және мәртебесі: • Күй талдауды орындау барысында файлдың ағымдағы күйін білдіреді • Мәртебе мінез-құлықты талдау нәтижесін немесе нәтиженің жоқтығын білдіреді • Басқару орталығының консолінде немесе үлгі бойынша есепте көрсетілетін тексерілген үлгілерге берілген мәртебе санатының болуы: • Жұқтырылмаған - Анықтау модульдері үлгіні зиянды ретінде сәйкестендірмейді. • Күдікті - Анықтау модулі файлдың мінез-құлқын күдікті, бірақ зиянды емес деп анықтады. • Зиянды - Файлдың мінез-құлқы зиянды деп саналады. • 2 минут ішінде пайдаланушының компаниясында қауіпсіздікті қамтамасыз ету үшін барлық өнімдерге тексерілген файлдар туралы нәтижелерді тарату функционалдығының болуы • Қауіпсіздікті қамтамасыз ету орталығының консоліне жіберілген барлық файлдар туралы тізімді ұсыну функционалдығының болуы. Таңдалған консоль бөлімінде жіберілген файлдар тізімін көруге болады. • Қауіпсіздікті қамтамасыз ету орталығының консоліне үлгілерді жіберуді баптау мүмкіндігі • Қауіпсіздікті қамтамасыз ету орталығының консолінде қауіпсіздікті қамтамасыз ету өнімдеріне арналған саясат үлгілері үшін ерекшеліктерді баптау және баптау мүмкіндігі. Вирусқа қарсы базаны жаңартуға қойылатын талаптар Жаңартылатын вирусқа қарсы деректер базасы келесі функционалдық мүмкіндіктерді жүзеге асыруды қамтамасыз етуі қажет: • трафикті үнемдеуге арналған жаңарту айнасын құру мүмкіндігінің іске асырылуы; • өнімдерін пайдаланғанда • Құжаттар (.docx, .xslx, .rtf және басқалар) • Орындалатын файлдар (.exe, .dll, .sys және басқа файлдар) • JAR, LNK, REG, MSI, SWF және басқалар • Сценарийлер (.bat, .cmd, .js, .vbs, .ps және басқалар) • Ole2 - пошта серверлерін қорғау өнімдерін пайдаланған кезде; • .hta • Пошта серверлерін қорғау жөніндегі өнімдермен пайдалану кезінде – құмсалғышта талдау кезінде шифрланған архивтер үшін парольдерді іріктеу функционалының болуы; • Бақыланатын үлгінің мінез-құлқының қысқаша сипаттамасы келтірілетін тексерілген үлгінің мінез-құлқы туралы есеп беру функционалдығының болуы. Файл туралы есепте келесі ақпарат болуы керек: • Файлды жіберген компьютердің аты; • файлды жіберген бастапқы компьютерде пайдаланушыны көрсету. Кейбір жағдайларда бұл жүйелік пайдаланушы болуы мүмкін. • Жіберу себебі (автоматты түрде, қолмен). • файлды алған бұлттың бөлігі көрсетілген; • Хеш SHA1 жіберілген файл. • Файл атауы және оның жіберушілердің файлдық жүйесіндегі толық жолы. • Файлдың көлемі. • Файл санаты (файл түрі). • Есепте параметрлердің болуы: Жағдайы және мәртебесі: • Күй талдауды орындау барысында файлдың ағымдағы күйін білдіреді • Мәртебе мінез-құлықты талдау нәтижесін немесе нәтиженің жоқтығын білдіреді • Басқару орталығының консолінде немесе үлгі бойынша есепте көрсетілетін тексерілген үлгілерге берілген мәртебе санатының болуы: • Жұқтырылмаған - Анықтау

	модульдері үлгіні зиянды ретінде сәйкестендірмейді. • Күдікті - Анықтау модулі файлдың мінез-құлқын күдікті, бірақ зиянды емес деп анықтады. • Зиянды - Файлдың мінез-құлқы зиянды деп саналады. • 2 минут ішінде пайдаланушының компаниясында қауіпсіздікті қамтамасыз ету үшін барлық өнімдерге тексерілген файлдар туралы нәтижелерді тарату функционалдығының болуы • Қауіпсіздікті қамтамасыз ету орталығының консоліне жіберілген барлық файлдар туралы тізімді ұсыну функционалдығының болуы. Таңдалған консоль бөлімінде жіберілген файлдар тізімін көруге болады. • Қауіпсіздікті қамтамасыз ету орталығының консоліне үлгілерді жіберуді баптау мүмкіндігі • Қауіпсіздікті қамтамасыз ету орталығының консолінде қауіпсіздікті қамтамасыз ету өнімдеріне арналған саясат үлгілері үшін ерекшеліктерді баптау және баптау мүмкіндігі. Вирусқа қарсы базаны жаңартуға қойылатын талаптар Жаңартылатын вирусқа қарсы деректер базасы келесі функционалдық мүмкіндіктерді жүзеге асыруды қамтамасыз етуі қажет: • трафикті үнемдеуге арналған жаңарту айнасын құру мүмкіндігінің іске асырылуы; • жаңарту айнасын ДК желісінде пайдаланылатын Windows/Linux операциялық жүйеге тәуелсіз, оның ішінде және ақырғы жұмыс станциясында AV-клиенттің көмегімен жаңартуды таратудың (HTTP және SMB) минимум екі жолы ретінде міндетті болумен құруға болады, айнаны активациялау үшін қосымша модулдерді, серверлерді және жұмыс станцияларын орнату талап етілмеуі қажет; • жаңарту типтері: вирустар сигнатурасының ДБ, бағдарламалық компоненттерді жаңарту, ядроны жаңарту; • айнаны жаңарту пакеттерін екі тәсілмен: HTTP протоколы бойынша (ұсынылады) және жалпы желілік дискінің (SMB) көмегімен жүктеуге болады; • Жаңартуды ақпараттарды электрондық тасушылармен (FDD\CD\DVD\ USB-drive) таратуға болады; • Электрондық сандық қол қою құралымен жаңартудың тұтастығына және дұрыстығына тексеру іске асырылады. Пайдалану құжаттарына қойылатын талаптар Барлық вирусқа қарсы бағдарламалық өнімдерге арналған пайдалану құжаты, оған басқару жүйесін қоса, орыс тіліндегі құжаттарды енгізуі қажет: оның ішінде: • пайдаланушының (әкімгердің) басшысы; • қашықтан әкімгерлеу құралының әкімгерге арналған басшылығы. Вирусқа қарсы құралдармен жеткізілетін құжаттар, вирустан қорғаудың тиісті құралдарын орнатуды, баптауды және пайдалану процестерін жете сипаттауы қажет. Техникалық қолдауға қойылатын талаптар Вирусқа қарсы бағдарламалық қамсыздандыруды техникалық қолдау: • Антивирустық бағдарламалық қамтамасыз етудің техникалық қолдауы орыс тілінде тәулік бойы, аптасына 7 күн, мереке және демалыс күндерін қоса алғанда (24/7 режимінде), электрондық пошта, Интернет желісі және телефон байланысы арқылы көрсетілуі тиіс. • ВҚ өндірушінің Web-сайты орыс тілінде болуы, техникалық қолдау көрсетуге, білім базасын толықтыруға арналған арнайы бөлімі мен орыс тілді форумы болуы қажет.

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)	Серверлік және клиенттік бөлігінің бағдарламалық жасақтама лицензияларын жаңарту шеңберіндегі қызметтерді сатып алу жеңімпазы болып айқындалған өнім беруші өз мамандарының күшімен және өз есебінен ұсынуы керек. Өз мамандарының күшімен келу, телефон және электронды пошта арқылы қызмет етілетін барлық бағдарламалық жасақтаманы теңшеу, орнату және функционал туралы кеңес беру мүмкіндігі болу керек.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Департамент полиции Атырауской области Министерства внутренних дел Республики Казахстан"
Наименование организатора	Государственное учреждение "Департамент полиции Атырауской области Министерства внутренних дел Республики Казахстан"
№ конкурса:	№ 17912320-1
Наименование конкурса:	Услуги по продлению лицензионного программного обеспечения
Номер лота:	№ 81448342-ОК1
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:	8973747.76
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	8973747.76
Срок оказания услуги:	по 31 декабря 2026 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Техническая спецификация на услуги по продлению лицензионного программного обеспечения (антивирус) Общие требования Антивирусная защита (АЗ) должна представлять собой масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети рабочих станций и серверов. В рамках всей организации должны использоваться единые антивирусные средства. Отдельно стоящие персональные компьютеры, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус). Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке. Для организаций имеющих офисы за границей должна иметься возможность выбора языка интерфейса консоли управления для подключения к серверу администрирования, без переустановки консоли и сервера для ИТ персонала родной язык которого отличается от русского. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке. Технические параметры программных средств антивирусной защиты должны соответствовать или превосходить следующие указанные параметры: Антивирусные средства и средства централизованного управления должны включать: • лицензионные файлы ключей для пакетов антивирусного программного обеспечения (АПО); при использовании схемы с несколькими серверами удаленного администрирования кластерная технология для организации связи между серверами не требуется дополнительных лицензий на связь между серверами. • программные средства антивирусной защиты рабочих станций, серверов и мобильных устройств (смартфонов, планшетов) ESET NOD32 для 700 пользователей. • агент администрирования для выполнения связи между сервером администрирования и защищаемыми узлами • программные средства централизованного управления, мониторинга и обновления на ОС Windows, Linux/BSD, Mac OS, мобильные ОС Android; • программные средства централизованного управления должны иметь WEB консоль для управления и формирования отчетов; • централизованное управление может осуществляться с любого устройства через Web - браузер; • программные средства централизованного управления могут устанавливаться на Windows и Linux платформы • обновляемые антивирусные базы данных и компоненты ядра антивирусной системы; • Прокси- сервер - компонент для обеспечения высокой масштабируемости решения и уменьшения нагрузки на центральный сервер администрирования • наличие инструмента для обнаружения неизвестных компьютеров, осуществляющего автоматический поиск ПК в локальной сети, без необходимости осуществлять их ручной поиск и добавление; • наличие различных вариантов установки агентов администрирования клиентской части антивирусного программного обеспечения такие как: удаленно или локально : - Push установка, - Установка через e-mail, - Установка с применением съемного носителя ,

	например USB, - Локальная установка; • эксплуатационную документацию на русском языке. • Наличие выделенного программного инструмента для управления лицензиями. С его помощью можно отслеживать лицензии, активированные модули и связанные с лицензиями события, такие как окончание срока действия, использование и авторизация. • Наличие выделенной утилиты для создания локального хранилища вирусных сигнатур, без использования сервера централизованного управления. • Наличие возможности организации двухфакторной аутентификации пользователей консоли сервера централизованного управления. • сервис дополнительного уровня безопасности продуктов включающий встроенную песочницу Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС: • Microsoft Windows Vista; • Microsoft Windows Vista x64; • Microsoft Windows 7 • Microsoft Windows 7 x64. • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows 10 Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей: • интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением; • резидентный антивирусный мониторинг; • возможность полностью скрыть интерфейс антивирусного ПО • антивирусное сканирование по команде пользователя или администратора; • антивирусное сканирование по расписанию; • антивирусное сканирование при определенных условиях: - после обновлений антивирусных баз данных; - каждый раз при запуске компьютера; - каждые сутки при первом запуске компьютера; - при успешном Интернет или VPN соединении; - вход пользователя; - при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени». - состояние простоя, автоматически сканирует локальные диски, если компьютер находится в состоянии простоя, в одном из следующих трех режимов: заставка, блокировка компьютера, выход пользователя • наличие задачи на выключение ПК по завершению сканирования • антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPs, POP3 и POP3s, а так же IMAP и IMAPs трафика. • наличие дополнительного модуля по защите документов Microsoft Office и сканировании проходящих через Internet Explorer файлов • защита от еще неизвестных вредоносных программ на основе эвристического анализа; • возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК: • обнаружение скрытых процессов; • возможность устанавливать только необходимые компоненты антивирусной защиты (модульная установка); • возможность отключения антивирусной защиты при необходимости; • антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE,

	DIET, EXEPACK и пр.; • антивирусная проверка и лечение файлов в архивах форматов ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE; • содержать настраиваемую систему предотвращения вторжений Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, изменения, а так же для мониторинга процессов, файлов и ключей реестра; • возможность работы HIPS по ряду заранее подготовленных режимов фильтрации; • обеспечивать защиту от хакерских атак, путем использования межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/HIPS) при работе в вычислительных сетях любого типа, включая беспроводные; • персональный файервол; • возможность настройки нескольких профилей файервола, с автоматическим переключением данных профилей, при выполнении определенных условий; • управление всем сетевым трафиком компьютера в обоих направлениях; • низкоуровневое сканирование трафика; • поддержка протокола IPv6; • поддержка встроенной песочницы для защиты от угроз нулевого дня; • модуль сканирования UEFI; • выделенный модуль защиты от вирусов шифраторов; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов, а также путем запрета всех веб-сайтов, кроме тех, которые внесены в список разрешенных; • активный режим фильтрации для приложений, а так же возможность отключения фильтрации или перевод в пассивный режим для исключенных приложений; • настраиваемый веб-контроль по категориям сайтов, позволяющий задавать правила применения политики использования сети Интернет на уровне пользователей или групп пользователей; • Наличие в модуле веб-контроля возможности кастомизации страницы предупреждения или блокирования • фильтрации для доверенных приложений; • сканирование из контекстного меню; • отключение фильтрации для доверенных веб-адресов; • отключение фильтрации для доверенных IP адресов; • возможность исключить из проверки доверенные процессы, хэш суммы, файлы и папки. • настройка нескольких профилей обновлений (например, для мобильных пользователей) с возможностью обновления из сети Интернет; • Наличие агента администрирования антивирусного программного обеспечения (АПО) для рабочих станций • наличие планировщика в клиенте антивирусного ПО; • возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы; • ядро и все основные модули продукта не требуют перезагрузки и активны сразу после установки; • наличие специализированной утилиты для сбора файлов журналов о конфигурации

	системы, установке и функционировании антивирусного пакета для ускорения решения проблем при возможных проблемах с антивирусным пакетом • наличие модуля сканирования в состоянии простоя, автоматически сканирует локальные диски, если компьютер находится в состоянии простоя, в одном из следующих трех режимов: заставка, блокировка компьютера, выход пользователя • возможность подключения уже установленных лицензий антивирусной защиты рабочих станций к серверу централизованного управления без необходимости удаления существующего пакета антивирусной защиты, путем установки агента администрирования ; • запуск обновления антивирусных баз данных после установки модемного соединения или VPN; • возможность создания задачи запуска приложения стороннего производителя в планировщике антивируса при определенных условиях или по временному интервалу; • защита на лету от вредоносных сценариев, загружаемых с Web-страниц • блокирование нежелательных и рекламных сообщений • самообучаемый антиспам; • защита почтовых клиентов: Microsoft Outlook, Outlook Express,Windows Mail, Windows Live Mail; • черные и белые списки антиспама, списки исключений • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • наличие функциональности использования общего локального кэша для повышения скорости сканирования в виртуализированных средах; • защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов; • Защита от эксплойтов: блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее неизвестных эксплойтов – угроз нулевого дня • наличие модуля сканирования памяти, который отслеживает поведение процессов и сканирует зловредные процессы, когда они снимают маскировку в памяти; • защита от ботнетов: помогает обнаруживать вредоносные программы, анализируя их схемы обмена данными и протоколы • регулировка распределения ресурсов рабочей станции между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; • настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта; • наличие модуля, позволяющего проводить автоматическое сканирование содержания подключаемых внешних устройств хранения данных, а так же применять расширенный анализ для запуска файлов с таких устройств; • наличие модуля, позволяющего настроить ограничения доступа (нет доступа, только чтение, полный доступ, предупреждение) для каждого пользователя или для группы пользователей как по типу устройства (CD/DVD/Blu-Ray, USB хранилища данных, USB принтеры, устройства обработки изображений, Устройства FireWire, кард ридеров, модемов, LPT\COM порты, Bluetooth устройства) так и по заданным атрибутам

	(производитель, модель, серийный номер) задавать одно правило на несколько устройств ; • интеграция с MS NAP и CISCO NAC; • возможность формирования аварийных дампов памяти, на случай сбоя приложения • возможность отката обновлений вирусных баз на предыдущие версии и приостановка их обновления с последующим автоматическим включением обновления через указанный промежуток времени; • наличие функциональности возобновлять прерванные загрузки баз данных сигнатур вирусов и модули продуктов при обновлении; • интеграция с центром безопасности Windows; • интеграция с центром обновления Windows , для установки патчей закрывающих обнаруженные уязвимости, с выбором необходимых обновлений от «необязательных» обновлений до «критических»; • настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи; • технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • проверка наличия актуальных обновлений системы; • наличие настраиваемой функции автоматического скрытия уведомлений при работе антивируса для приложений, работающих в полноэкранном режиме, т.е. при работе приложения в полноэкранном режиме на экран не выводятся информационные уведомления о работе антивирусного программного обеспечения; • наличие множества путей уведомления администраторов о важных событиях, происходящих на рабочих станциях (почтовое сообщение, всплывающее окно, запись в журнал событий); • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отчуждаемых носителях информации; • экспорт логов и отчетов в форматы XML,TXT, DAT, DMP; • наличие облачной технологии детектирования неизвестных угроз, контроль приложений на основе репутационного сервиса; • наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную; • возможность создания дисков аварийного восстановления; • экономия электроэнергии в режиме автономного питания; • системные требования не должны превышать: 300мб RAM, HDD 1гб, Processor Intel или AMD, одноядерный, x86 или x64 1ГГц. • размер дистрибутива антивирусного пакета не должен превышать – 165 Мб. Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС: • Microsoft Windows Server 2008 (x86 и x64) • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2008 x64 R2 SP1 / x64 R2 CORE • Microsoft Windows Server 2008 x86 SP2 / x64 SP2 CORE • Microsoft Windows Server 2012 x64 / x64 CORE • Microsoft Windows Server

	2012 x64 R2 / x64 R2 CORE • Microsoft Windows Hyper-V Server 2008 R2 • Microsoft Windows Hyper-V Server 2012 • Microsoft Windows Hyper-V Server 2012 R2 Серверы Storage, Small Business и MultiPoint: • Microsoft Windows Storage Server 2008 R2 Essentials с пакетом обновления 1 • Microsoft Windows Storage Server 2012 • Microsoft Windows Storage Server 2012 R2 • Microsoft Windows Small Business Server 2008 (x64) • Microsoft Windows Small Business Server 2011 (x64) • Microsoft Windows Server 2012 Essentials • Microsoft Windows Server 2012 R2 Essentials • Microsoft Windows MultiPoint Server 2010 • Microsoft Windows MultiPoint Server 2011 • Microsoft Windows MultiPoint Server 2012 Программные средства антивирусной защиты файловых серверов под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей: • интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением; • резидентный антивирусный мониторинг; • антивирусное сканирование по команде пользователя или администратора; • антивирусное сканирование по расписанию; • антивирусное сканирование при определенных условиях: - после обновлений антивирусных баз данных; - каждый раз при запуске компьютера; - каждые сутки при первом запуске компьютера; - при успешном Интернет или VPN соединении; - вход пользователя; - при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени». • антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPs, а так же POP3 и POP3s трафика • антивирусное сканирование Hyper-V на наличие вирусов на безагентной основе • защита от еще неизвестных вредоносных программ на основе эвристического анализа; • содержать настраиваемую систему предотвращения вторжений Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, изменения, а так же для мониторинга процессов, файлов и ключей реестра; • возможность работы HIPS по ряду заранее подготовленных режимов фильтрации • возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК: • возможность исключить определенные процессы приложений, хэш суммы из сканирования на наличие вирусов; • обнаружение руткитов (скрытых файлов/системных аномалий); • антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.; • антивирусная проверка и лечение файлов в архивах форматов ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность создания задачи запуска приложения стороннего производителя в планировщике антивируса; • защита на лету от вредоносных сценариев, загружаемых с Web-страниц; • возможность настройки параметров антивирусного пакета из интерфейса командной строки • функция автоматического

	обнаружение и исключения файлов на сервере, имеющих критическое значение для бесперебойной работы; • возможность задать количество модулей сканирования для увеличения скорости сканирования; • возможность управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов, а также путем запрета всех веб-сайтов, кроме тех, которые внесены в список разрешенных; • активный режим фильтрации для приложений, а так же возможность отключения фильтрации или перевод в пассивный режим для исключенных приложений; • сканирование из контекстного меню; • отключение фильтрации для доверенных веб-адресов; • многопоточное сканирование; • настройка нескольких профилей обновлений (например для мобильных пользователей) с возможностью обновления из интернета. • наличие планировщика в антивирусном пакете . • наличие агента администрирования антивирусного программного обеспечения (АПО) для файловых серверов • возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы; • ядро и все основные модули продукта не требуют перезагрузки и активны сразу после установки; • возможность подключения уже установленных лицензий антивирусной защиты рабочих станций к серверу централизованного управления без необходимости удаления существующего пакета антивирусной защиты, путем установки агента администрирования ; • наличие облачной технологии детектирования неизвестных угроз, контроль приложений на основе репутационного сервиса; • запуск обновления антивирусных баз после установки модемного соединения или VPN; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • наличие специализированной утилиты для сбора файлов журналов о конфигурации системы, установке и функционировании антивирусного пакета для ускорения решения проблем при возможных проблемах с антивирусным пакетом • наличие функциональности использования общего локального кэша для повышения скорости сканирования в виртуализированных средах; • защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов; • Защита от эксплойтов: блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее неизвестных эксплойтов – угроз нулевого дня • поддержка встроенной песочницы для защиты от угроз нулевого дня; • модуль сканирования UEFI; • выделенный модуль защиты от вирусов шифраторов; • модуль защиты от сетевых атак; • модуль защиты от ботнетов; • наличие модуля сканирования

	памяти, который отслеживает поведение процессов и сканирует зловредные процессы, когда они снимают маскировку в памяти; • регулировка распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; • настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта; • блокировка сменных носителей информации и устройств (USB); • наличие модуля, позволяющего настроить ограничения доступа (нет доступа/только чтение/полный доступ/предупреждение) для каждого пользователя или для группы пользователей как по типу устройства (CD/DVD/Blu-Ray, USB хранилища данных, USB принтеры, устройства обработки изображений, Устройства FireWire, кард ридеров, модемов, LPT\COM порты, Bluetooth устройства) так и по заданным атрибутам (производитель/модель/серийный номер) задавать одно правило на несколько устройств ; • интеграция с центром безопасности Windows; • интеграция с центром обновления Windows, для установки патчей закрывающих обнаруженные уязвимости, с выбором необходимых обновлений от «необязательных» обновлений до «критических»; • поддержка Windows Management Instrumentation • настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи; • поддержка кластерных систем с возможностью автоматического объединения антивирусного ПО (автоматическая синхронизация конфигурации ПО на кластерах) • технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • проверка наличия актуальных обновлений операционной системы; • полноценная работа без графического интерфейса, администрирование и конфигурирование АПО через командную строку; • возможность автоматизации работы за счет выполнения сценариев, позволяющих конфигурировать АПО и выполнять какие-либо действия; • автоматическое скрытие уведомлений при работе антивируса в полноэкранном режиме; • наличие настраиваемой функции автоматического скрытия уведомлений при работе антивируса для приложений, работающих в полноэкранном режиме; • наличие множества путей уведомления администраторов о важных событиях, происходящих на серверах (почтовое сообщение, всплывающее окно, запись в журнал событий); • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отчуждаемых носителях информации; • наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную; • возможность создания дисков аварийного восстановления; • размер дистрибутива антивирусного пакета не должен превышать – 127 Мб. Требования к средствам антивирусной защиты мобильных устройств: Программные средства антивирусной защиты смартфонов

	должны обеспечивать следующую функциональность: • возможность проведения аудита безопасности устройства с генерацией отчета; • постоянная защиту файловой системы смартфона, планшета; • проверка всех приложений, файлов, папок и карты памяти в режиме реального времени; • проверка объектов файловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию; • надежное изолирование зараженных объектов в карантинном хранилище; • обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов; • блокирование нежелательных SMS и MMS сообщений; • контроль приложений для отслеживания установленных приложений, блокировать доступ к определенным приложениям и снижать степень риска, предлагая пользователям удалять некоторые программы • задание минимальных уровней безопасности и сложность кодов разблокировки экрана; • указание максимального количества неудачных попыток разблокировки; • указание максимального срока действия для кода разблокировки экрана; • настройка таймера блокировки экрана; • ограничить использование камеры. • защита от фишинга: защита пользователей от попыток получить пароли, банковские данные и прочую конфиденциальную информацию незаконными веб-сайтами, выдающими себя за законные • центр уведомлений: предоставляет сведения о разных событиях, о причинах их несоответствия корпоративным политикам и о том как эту несовместимость устранить • защита от кражи и утери смартфона. Обеспечить возможность удаленной блокировки мобильного устройства; • возможность дистанционно удалить информацию со смартфона; • возможность определить доверенную SIM-карту; • автоматическая скрытая отправка уведомления посредством SMS-сообщения, с предупреждением об использовании не доверенной SIM-карте. Так же сообщение должно включать информацию, необходимую для идентификации злоумышленника: телефонный номер текущей SIM-карты, номер IMSI и номер IMEI телефона. • расширенный сброс до заводских установок: все доступные на устройстве данные будут удалены (заголовки файлов будут уничтожены). Кроме того, на телефоне будут восстановлены заводские настройки по умолчанию • возможность включить сирену:Потерянное устройство блокируется и начинает издавать очень громкий звук, даже если звук на устройстве отключен • Наличие встроенного агента администрирования антивирусного программного обеспечения (АПО) Требования к системе управления антивирусной защитой Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей: • масштабируемое решение: масштабирование производится за счет использования прокси серверов • интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением; • Прокси- сервер - компонент для обеспечения высокой масштабируемости решения и уменьшения нагрузки на центральный сервер администрирования • наличие инструмента для

	обнаружения неизвестных компьютеров, осуществляющий автоматический поиск ПК в локальной сети, без необходимости осуществлять их ручной поиск и добавление; • централизованная установка/обновление/удаление программных средств антивирусной защиты, настройки, администрирования; • централизованный сбор информации и создание отчетов о состоянии антивирусной защиты; • защищенное соединение между сервером и клиентом; • программные средства централизованного управления должны иметь WEB консоль для управления и формирования отчетов; • централизованное управление может осуществляться с любого устройства через Web - браузер; • создание отчетов в наглядном графическом виде; • экспорт логов и отчетов в форматы HTML,TXT, CSV, PDF; • наличие модуля поддержки SIEM; • предварительная настройка политик для групп или клиентов (профили обновлений, запрещенные сайты, расписание планировщика и т.д.); • возможность отправки сообщений, как на мобильные устройства, так и на персональные компьютеры; • возможность удаленного создания журнала аудита безопасности с мобильного устройства • возможность установки пользовательских приложений; • наличие различных вариантов установки агентов администрирования клиентской части антивирусного программного обеспечения такие как: удаленно или локально : - Push установка, - Установка через e-mail, - Установка с применением съемного носителя , например USB, - Локальная установка; • наличие возможности автоматически выбирать соответствующий установочный пакет агента для операционных систем или в ручном режиме. • настройка политик безопасности для клиентов; • возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы; • возможность удаленного запуска определенного сценария на конечных клиентах, предназначенного для удаления/изменения критических объектов системы. • отсутствие необходимости перезагрузки ПК после установки системы управления антивирусной защиты; • автоматизированное обновление программных средств антивирусной защиты и антивирусных баз; • возможность произвести быстрый откат обновлений сигнатурных баз для отдельных компьютеров или групп; • доставка обновлений на рабочие места пользователей сразу после их получения; • централизованный карантин; • возможность создания групп управляемых компьютеров как вручную, так и автоматически на основе структуры Active Directory; • возможность синхронизации с Active Directory как по расписанию, так и вручную; • автоматический поиск незащищенных рабочих станций с учетом топологии сети; • аудит изменений в настройках сервера по учетным записям; • построение многоуровневой системы управления с возможностью настройки

	ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на носителях информации; • механизм оповещения о событиях в работе установленных приложений антивирусной защиты и возможность настройки рассылки почтовых уведомлений о них; • наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную; • возможность создания динамических групп, в которые динамически будут включаться клиентские станции при соответствии условиям данных групп; • работа со статическими и динамическими группами • различные варианта уведомлений администратора сети (по e-mail,использование SNMP-ловушки); • возможность создания резервных копий содержимого базы данных и настроек сервера; • возможность подключения к консоли сервера удаленного администрирования с использованием доменных имени пользователя и пароля; • администрирование серверов и рабочих станций Windows, Linux\BSD, а так же решений для защиты мобильных ОС (Android); • наличие функции пробуждения по локальной сети Wake on LAN • возможность автоматического определения «клонированных машин» с помощью сложной логики обнаружения отпечатков оборудования. • наличие протокола для репликации, с использованием «PNS» (Push Notification Service) и поддержкой многоадресных вызовов для WOL. • функционал для инвентаризации оборудования. • наличие функции быстрого отключения или включения уведомлений на выбранных компьютерах для прерывания или возобновления обмена данными с сервером администрирования • поддержка баз данных MS SQL, MySQL; • программные средства централизованного управления могут устанавливаться на Windows и Linux платформы • программные средства должны поддерживать установку на отказоустойчивые кластеры Windows и Linux платформ • сервер удаленного администрирования может быть установлен и должен поддерживать операционные системы Windows Server: o Windows Server 2003 x86 SP2 /x64 SP2 o Windows Server 2003 x86 R2 SP2 /x64 R2 SP2 o Windows Server 2008 x64 R2 SP1 / x64 R2 CORE o Windows Server 2008 x86 SP2 / x64 SP2 o Windows Server 2012 x64 / x64 CORE o Windows Server 2012 x64 R2 / x64 R2 CORE o Microsoft SBS 2003 x86 SP2 / x86 R2 o Microsoft SBS 2008 x64 SP2 o Microsoft SBS 2011 x64 Standard / x64 Essential Linux: o Ubuntu 12.04 LTS x86 Desktop / Server o Ubuntu 12.04 LTS x64 Desktop / Server o Ubuntu14.04. LTS x86 Desktop / Server o Ubuntu 14.04 LTS x64 Desktop / Server o RHEL Server 6 x86 / x64 o RHEL Server 7 x86 / x64 o CentOS 6 x86 / x64 o CentOS 7 x86 / x64 o SLED 11 x86 / x64 o SLES 11 x86 /x64 o OpenSUSE 13 x86 / x64 o Debian 7 x86 / x64 o Fedora 19 x86 / x64 • Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий: o VMware vSphere/ESXi (версии 5.0 и новее) o VMware Workstation (версии 9 и новее) o VMware Player (версии 7 и новее) o Microsoft

	Hyper-V (Server 2012 и 2012 R2) о Oracle VirtualBox (версии 4.3.24 и новее) Наличие выделенного программного инструмента для управления лицензиями. С его помощью можно отслеживать лицензии, активированные модули и связанные с лицензиями события, такие как окончание срока действия, использование и авторизация. Работа с инструментом под разными ролями как владелец лицензии или как администратор безопасности. Возможность выполнять следующие действия: • просматривать состояние лицензий в реальном времени; • отслеживать отдельные устройства (и при этом их отключать); • настраивать уведомления, связанные с событиями лицензии; • хранить лицензии одновременно в старой и новой формах в смешанных средах; • обменивать ключи лицензий на сообщения электронной почты и пароли, с помощью которых также можно активировать программы; • назначать несколько лицензий на одну учетную запись; • разрешать другим лицам использовать лицензии (активировать их); • настраивать уведомления для более удобного отслеживания состояния лицензии; • наличие функции синхронизации с сервером централизованного управления. • наличие выделенной утилиты для мигрирования с более ранних версий антивирусного программного обеспечения с сохранением настроек политик и информационной базы журналов событий. • наличие выделенной утилиты для создания локального хранилища вирусных сигнатур, без использования сервера централизованного управления. • наличие возможности организации двухфакторной аутентификации пользователей консоли сервера централизованного управления. Поддержка двухфакторной аутентификации для 10 пользователей консоли сервера централизованного управления. При использовании данной функциональности должно быть использовано решение двухфакторной аутентификации того же производителя, что и сам пакет антивирусного программного обеспечения. • наличие возможности деактивации лицензий на узлах через создание заданий на сервере управления. Сервис дополнительного уровня безопасности продуктов для защиты рабочих станций, файловых и почтовых серверов с помощью встроенной песочницы на основе технологий машинного обучения для обнаружения новых, ранее неизвестных угроз. В сервисе должна быть реализована следующая функциональность: • Детектирование на основе анализа поведения • Машинное обучение • Обнаружение угроз нулевого дня • Встроенная песочница Сервис на основе технологий машинного обучения для обнаружения новых, ранее неизвестных угроз поставляется в составе решения по антивирусной защите рабочих станций, файловых серверов локальной сети заказчика. • Наличие поддержки антивирусными продуктами дополнительной функциональности, активируемой отдельной лицензией. Сервис предназначен для продуктов того же производителя антивирусного обеспечения, что и сам сервис. Сервис должен активироваться и управляться из центра обеспечения безопасности системы. • Сервис должен поддерживать работу с антивирусными решениями по защите рабочих станций, файловых серверов и почтовых серверов. • Для

	работы с сервисом необходим только доступ в сеть интернет, никаких аппаратных средств в сети заказчика не требуется. Сервис должен обеспечивать: • Многоуровневую защиту - иметь не менее 3 моделей машинного обучения. Система выполняет работу с образцами в виртуальной среде или в песочнице. Система моделирует поведение пользователей, чтобы обмануть образцы вредоносных программ и использует модели нейронных сетей Deep Learning для сравнения поведения образцов с поведением всех известных образцов вредоносных программ. • Детальный обзор - Каждый изучаемый образец отображается в консоли центра безопасности, где наглядно и удобно представлена детальная информация о его характеристиках и происхождении. • Высокую скорость анализа – предоставлять анализ 90% неизвестных образцов в течение 5 минут • Мобильность – наличие возможности анализа файлов вне зависимости от местонахождения пользователей в корпоративной сети или за ее пределами. • Наличие возможности отправки подозрительных файлов вручную или автоматически на основе конфигурации политики. • Возможность отправки файлов вручную из веб-консоли Центра обеспечения безопасности или с клиентских компьютеров с активированным сервисом. • Возможность управлять действиями сервиса через API Центра обеспечения безопасности • Наличие возможности отправки больших файлов объемом до 64 Мб • Поддерживаемые типы файлов для отправки на проверку: • Документы (.docx, .xslx, .rtf и др.) • Исполняемые файлы (файлы .exe, .dll, .sys и др.) • JAR, LNK, REG, MSI, SWF и др • Сценарии (.bat, .cmd, .js, .vbs, .ps и др.) • Ole2 - при использовании с продуктами по защите почтовых серверов • .hta • Наличие функциональности предоставления отчета о поведении проверенного образца, в котором будет приведено краткое описание поведения наблюдаемого образца. В Отчете о файле должна содержаться следующая информация: • Имя компьютера, отправившего файл • указание Пользователя на исходном компьютере, отправившего файл. В некоторых случаях это может быть системный пользователь • Причина отправки (автоматически, вручную). • указана Часть облака, получившая файл • Хеш SHA1 отправленного файла. • Имя файла и его полный путь в файловой системе отправителей. • Размер файла. • Категория файла (тип файла). • Наличие в отчете параметров: Состояние и Статус: • Состояние означает текущее состояние файла в процессе выполнения анализа • Статус означает результат анализа поведения или отсутствие результата • Наличие категории статуса, присвоенного проверенным образцам, которое отображается в консоли центра управления или в отчете по образцу: • Не заражено - Модули обнаружения не идентифицируют образец как вредоносный. • Подозрительный - Модуль обнаружения определил поведение файла как подозрительное, но не вредоносное. • Вредоносный - Поведение файла считается вредоносным. • Наличие функциональности распространения результатов о проверенных файлах во все продукты для обеспечения безопасности в компании пользователя в течение не более 2 минут •

	Наличие функциональности предоставления списка о всех переданных файлах в консоль Центра обеспечения безопасности. Можно просмотреть список отправленных файлов в выделенном разделе консоли. • Возможность настройки отправки образцов в консоли Центра обеспечения безопасности • Возможность настройки исключений для образцов и настройки политик для продуктов обеспечения безопасности в консоли Центра обеспечения безопасности. Требования к обновлению антивирусных баз Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: • реализована возможность создания зеркала обновлений для экономии трафика; • зеркало обновлений можно создать на любом ПК сети не зависимо от используемой операционной системы Windows/Linux , в том числе и на конечной рабочей станции при помощи AV-клиента с обязательным наличием как минимум двух путей раздачи обновлений (HTTP и SMB), для активации зеркала не должна требоваться установка дополнительных модулей, как на сервер, так и на рабочую станцию; • типы обновлений: обновление БД сигнатур вирусов, программных компонентов, обновление ядра; • пакеты обновления зеркала можно загружать двумя способами: по протоколу HTTP (рекомендуется) и с помощью общего сетевого диска (SMB); • обновления можно распространять на электронных носителях информации (FDD\CD\DVD\ USB-drive); • осуществляется проверка целостности и подлинности обновлений средствами электронной цифровой подписи. Требования к эксплуатационной документации Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы на русском языке, в том числе: • руководство пользователя (администратора); • руководство администратора средств удаленного администрирования. 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: • Техническая поддержка антивирусного программного обеспечения должна предоставляться на русском языке круглосуточно, 24 часа в сутки, 7 дней в неделю, включая праздничные и выходные дни (режим 24/7), посредством электронной почты, сети Интернет и телефонной связи. • Web-сайт производителя А3 должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний и русскоязычный форум.

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, определенный победителем закупки должен силами своих специалистов и за свой счет оказать все услуги в рамках продления лицензий программного обеспечения, как серверной его части, так и клиентской. Должен иметь возможность проведения консультаций по функционалу, настройке, установке, внедрению и сопровождению всего обсуживаемого ПО, силами своих специалистов, с выездом, по телефону и электронной почте.