**ESET NOD32 Smart Security Business Edition антивирустық бағдарламалық қамтамасыз ету пайдаланушылары санының көбею мүмкіндігімен ұзарту**

**қызметтерін мемлекеттік сатып алу бойынша**

**ТЕХНИКАЛЫҚ ЕРЕКШЕЛІК**

|  |  |  |
| --- | --- | --- |
| **Р/р №** | **Құрылымы** | **Ескертпе** |
| 1. | Тауарлардың, қызметтердің, жұмыстардың атауы | **ESET NOD32 Smart Security Business Edition антивирустық бағдарламалық қамтамасыз ету пайдаланушылары санының көбею мүмкіндігімен ұзарту** |
| 2. | Кепілдікмерзімі (айлар) | **Лицензияның қолданылу мерзімі -** 12 ай |
| 3. | Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы | **Бағдарламаға және қорғалатын объектілердің санына қойылатын талаптар:****ESET NOD32 Smart Security Business Edition антивирустық бағдарламасын ұзарту. Қорғалатын объектілердің саны – 800.**Вирусқа қарсы қорғау (ВҚ) жергілікті желідегі жұмыс станциялары мен серверлердің тұрақты жұмысын қамтамасыз ететін ауқымды шешім болуы керек. (ВҚ) шеңберінде бірыңғай вирусқа қарсы құралдарды пайдалану керек. Вирусқа қарсы қорғаудың бірыңғай жүйесіне қосылмаған дербес компьютерлер зиянды бағдарламалардың (антивирустық) барлық түрлерінен қорғауды қамтитын интеграцияланған бағдарлама өнімі арқылы қорғалуы тиіс.Барлық антивирустық құралдардың, соның ішінде басқару құралдарының бағдарламалық интерфейсі орыс тілінде болуы керек. Барлық антивирустық құралдар, соның ішінде басқару құралдары орыс тілінде контекстік анықтамалық жүйеге ие болуы керекВирусқа қарсы бағдарламалық құралдарының техникалық параметрлері төмендегі көрсетілген параметрлерге сәйкес келуі немесе одан асуы керек:**Антивирустық құралдар және орталықтандырылған басқару құралдары мыналарды қамтуы керек:*** антивирустық бағдарламалық жасақтама пакеттеріне арналған лицензиялық кілт файлдары (АБЖ); бірнеше қашықтағы әкімшілік серверлері бар схеманы пайдаланған кезде серверлер арасындағы байланысты ұйымдастыру үшін кластерлік технология серверлер арасындағы байланыс үшін қосымша лицензияларды талап етпейді.
* жұмыс стансаларының, серверлер мен мобильді құрылғылардың (смартфондар, планшеттер) антивирустық қорғауға арналған бағдарламалық құралдар
* әкімшілендіру сервері мен қорғалған түйіндер арасындағы байланыс үшін әкімшілендіру агенті
* Windows, Linux / BSD, MacOS ОЖ, Android мобильді ОЖ орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары;
* Басқарудың орталықтандырылған бағдарламалық құралдарында есептерді басқару және жасау үшін WEB консолы болуы керек;
* орталықтандырылған басқару Web-браузер арқылы кез-келген құрылғыдан орындалуы мүмкін;
* орталықтандырылған басқару бағдарламалық құралдарын Windows және Linux платформаларында орнатуға болады
* жаңартылатын вирусқа қарсы деректер базасы және вирусқа қарсы жүйе ядросының компоненттері
* Прокси-сервер - шешімнің жоғары ауқымдылығын қамтамасыз ететін және орталық әкімшілендіру серверіне жүктемені азайтатын компонент
* жергілікті желіде ДК автоматты түрде іздейтін белгісіз компьютерлерді қолмен іздеуді және қосуды қажет етпестен табуға арналған құралдың болуы
* антивирустық бағдарламалық қамтамасыз етудің клиенттік бөлігінің әкімшілендіру агенттерін орнатудың әр түрлі нұсқаларының болуы:

қашықтан немесе жергілікті:- Push орнату;- e-mail арқылы орнату;- USB сияқты алынбалы тасымалдаушыны пайдалана отырып орнату;- Жергілікті орнату;* Лицензияларды басқару үшін арнайы бағдарламалық құралдың болуы. Оның көмегімен лицензияларды, белсендірілген модульдерді және қолданылу мерзімінің аяқталуы, пайдалану және авторизация сияқты лицензиялармен байланысты оқиғаларды бақылауға болады.

Microsoft Windows тобының ОЖ басқаруындағы жұмыс стансаларының вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар.Microsoft Windows тобының ОЖ басқаруындағы жұмыс стансаларының вирусқа қарсы қорғау бағдарламалық құралдары келесі OЖ нұсқаларында жұмыс істеуі керек:* Microsoft Windows 7
* Microsoft Windows 7 x64.
* Microsoft Windows 8
* Microsoft Windows 8.1
* Microsoft Windows 10
* Microsoft Windows 11

Microsoft Windows тобының ОЖ басқаруындағы жұмыс стансаларының вирусқа қарсы қорғау бағдарламалық құралдары келесі функционалдық мүмкіндіктерді жүзеге асыруды қамтамасыз етуі керек:* вирусқа қарсы бағдарламалық қамтамасыз ету интерфейсі сенсорлы экрандар мен жоғары ажыратымдылықты экрандарды қолдауды қамтамасыз етуі керек;
* резиденттік антивирустық мониторинг;
* пайдаланушы немесе әкімші пәрмені арқылы антивирустық сканерлеу;
* кесте бойынша антивирустық сканерлеу;
* белгілі бір жағдайларда антивирустық сканерлеу:

- вирусқа қарсы дерекқорды жаңартқаннан кейін;- компьютерді әр іске қосу кезінде;- әр күн, компьютерді бірінші рет іске қосу кезінде;- табысты Интернет немесе VPN байланысы кезінде;- Пайдаланушының кіруі;- күдікті белсенділік анықталған кезде, соның ішінде «нақты уақыт режимінде қорғау» белсенді модулін қоса алғанда.* сканерлеу аяқталғаннан кейін ДК өшіру тапсырмасының болуы
* трафикті келесі хаттамалар бойынша антивирустық сканерлеу: FTP, HTTP және HTTP, POP3 және POP3, сонымен қатар трафиктің IMAP және IMAPs.
* Microsoft Office құжаттарын қорғау және Internet Explorer арқылы өтетін файлдарды сканерлеу үшін қосымша модульдің болуы
* эвристикалық талдауға негізделген белгісіз зиянды бағдарламалардан қорғау;
* ДК-да орналасуына қарамастан, белгілі бір қауіптерге ерекше жағдайларды қосу мүмкіндігі:
* жасырын процестерді анықтау;
* вирусқа қарсы қорғаудың тек қажетті құрамдас бөліктерін (модульді орнату) орнату мүмкіндігі;
* қажет болған жағдайда вирусқа қарсы қорғауды өшіру мүмкіндігі;
* PKLITE, LZEXE, DIET, EXEPACK сияқты және т.б. бағдарламалармен жинақталған 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 форматтарындағы мұрағаттардағы файлдарды вирусқа қарсы тексеру және емдеу;
* сыртқы әсер ету, өзгерту әрекеттерін болдырмауға, сондай-ақ процестерді, файлдарды және тізілім кілттерін бақылауға арналған Host Intrusion Prevention System (HIPS) теңшелетін басып кіруді болдырмау жүйесінің болуы;
* алдын ала дайындалған сүзгілеу режимдерінің бірқатарында HIPS жұмыс істеу мүмкіндігі;
* сымсыз желілерді қоса алғанда, кез келген түрдегі есептеу желілерінде жұмыс істеу кезінде басып кіруді анықтау және алдын алу жүйесі (IDS/HIPS) бар желіаралық экранды пайдалану арқылы хакерлік шабуылдардан қорғауды қамтамасыз ету;
* жеке файервол;
* белгілі бір шарттарды орындау кезінде профиль деректерін автоматты түрде ауыстыра отырып, бірнеше файервол профильдерін теңшеу мүмкіндігі;
* екі бағытта да компьютердің барлық желілік трафигін басқару;
* төмен деңгейлі трафикті сканерлеу;
* IPv6 протоколын қолдау;
* тапсырмаларды кесте бойынша және / немесе операциялық жүйе жүктелгеннен кейін дереу іске қосу;
* бұғатталған немесе рұқсат етілген веб-сайттардың тізімін жасау арқылы, сондай-ақ рұқсат етілген тізімге енгізілгендерден басқа барлық веб-сайттарға тыйым салу арқылы веб-ресурстарға қол жеткізуді басқару мүмкіндігі;
* қосымшалар үшін белсенді сүзгілеу режимі, сонымен қатар сүзгілеуді өшіру немесе шығарылған қосымшалар үшін пассивті режимге ауыстыру мүмкіндігі;
* пайдаланушылар немесе пайдаланушылар топтары деңгейінде Интернетті пайдалану саясатын қолдану ережелерін орнатуға мүмкіндік беретін сайттар санаттары бойынша теңшелетін веб-бақылау;
* сенімді қосымшаларға арналған сүзгілеу;
* контекстік мәзірден сканерлеу;
* сенімді веб-мекенжайлар үшін сүзгілеуді өшіру;
* сенімді IP мекенжайлар үшін сүзгілеуді өшіру;
* сенімді процестерді, файлдарды және қапшықтарды тексеруден шығару мүмкіндігі.
* Интернет желісінен жаңарту мүмкіндігі бар бірнеше жаңарту профильдерін (мысалы, мобильді пайдаланушылар үшін) теңшеу;
* жұмыс стансалары үшін вирусқа қарсы бағдарламалық жасақтаманы әкімшілендіру агентінің (AБЖ) болуы;
* вирусқа қарсы БЖ клиентінде жоспарлаушының болуы;
* өзгерістерді бақылау және оларды уақыт аралығындағы суреттер арқылы автоматты түрде салыстыру мүмкіндігімен ДК жай-күйі туралы, орнатылған қосымшалар, қызметтер, желілік қосылымдар және т. б. туралы жалпы ақпаратты бір орталықтан көру мүмкіндігі, сондай-ақ жүйенің дұрыс жұмысын қалпына келтіретін өзгерістер (процестер мен драйверлерді тоқтату, тізілім жазбалары мен жүйелік файлдарды жою және қалпына келтіру) енгізу мүмкіндігі;
* ядро және барлық негізгі өнім модульдін қайта жүктеуді қажет етпейді және орнатудан кейін бірден белсенді болады;
* вирусқа қарсы пакеті бар ықтимал проблемаларды шешуді тездету үшін антивирустық пакеттің конфигурациясы, орнату және жұмыс істеуі туралы журнал файлдарын жинауға арналған мамандандырылған утилитаның болуы;
* бос тұру күйінде сканерлеу модулінің болуы, егер компьютер бос тұрған жағдайда, жергілікті дискілерді автоматты түрде сканерлейді
* әкімшілендіру агентін орнату арқылы бұрыннан орнатылған жұмыс стансасының вирусқа қарсы қорғау лицензияларын орталықтандырылған басқару серверіне вирусқа қарсы қорғау пакетін жою қажеттілігінсіз қосу мүмкіндігі;
* модем қосылымын немесе VPN орнатқаннан кейін вирусқа қарсы дерекқордың жаңартылуын іске қосу;
* белгілі бір жағдайларда немесе уақыт аралығындағы антивирустық жоспарлаушыда үшінші тарап қосымшаларын іске қосу апсырмасын жасау мүмкіндігі;
* Web-беттерден жүктелетін зиянды сценарийлерден жылдам қорғау;
* қалаусыз және жарнамалық хабарламаларды бұғаттау;
* өзін-өзі үйрететін анти-спам;
* Пошталық клиенттерді қорғау: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail, Mozilla Thunderbird;
* Қара және ақ антиспамдардың тізімі, ерекше тізімдер;
* жағдайы соңғы тексеру уақытынан бері өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету;
* виртуалданған орталарда сканерлеу жылдамдығын арттыру үшін жалпы жергілікті кэшті пайдаланудың функционалдық мүмкіндігі;
* фишингтен қорғау: құпиясөздерді және басқа да құпия ақпаратты алу әрекеттерінен қорғайды, қалыпты веб-сайттар нысанын алатын зиянды веб-сайттарға кіруді болдырмайды;
* эксплойттардан қорғау: эксплойт-блокатор процестердің мінез-құлқын бақылайды және мақсатты шабуылдарға және бұрын белгісіз эксплойттар - нөлдік күннің қауіп-қатеріне тән күдікті әрекеттерді анықтайды;
* жадтағы бүркемені алып тастаған кезде процестердің әрекетін бақылайтын және зиянды процестерді сканерлейтін жадты сканерлеу модулінің болуы;
* ботнеттерден қорғау: зиянды бағдарламаларды олардың деректер алмасу схемалары мен хаттамаларын талдай отырып анықтауға көмектеседі;
* жұмыстың басымдылығына байланысты антивирус пен басқа қосымшалар арасында жұмыс стансасының ресурстарын бөлуді реттеу: фондық режимде антивирустық сканерлеуді жалғастыру мүмкіндігі;
* Параметрлер бойынша сканерлеу шектерін теңшеу – қабатталым тереңдігі (мұрағаттар), объектінің көлемі және объектінің сканерлеу уақыты;
* қосылатын сыртқы сақтау құрылғыларының мазмұнын автоматты түрде сканерлеуге, сондай-ақ осындай құрылғылардан файлдарды іске қосу үшін кеңейтілген талдауды қолдануға мүмкіндік беретін модульдің болуы;
* әрбір пайдаланушы үшін немесе пайдаланушы тобы үшін құрылғы түрі бойынша да (CD/DVD/Blu-Ray, USB деректер қоймасы, USB принтерлер, кескінді өңдеу құрылғылары, FireWire құрылғылары, карт ридерлер, модемдер, LPT\COM порттары, Bluetooth құрылғылары) кіру шектеулерін ( қол жетімділік жоқ, тек оқу, толық қол жетімділік) берілген атрибуттар бойынша да (өндіруші, модель, сериялық нөмір) бір ережені бірнеше құрылғыға беретін қол жетімділік шектеулерін реттеуге (қол жетімділік жоқ, тек оқу, толық қол жетімділік) мүмкіндік беретін модульдің болуы;
* MSNAP және CISCONAC-пен интеграция;
* істен шығуы жағдайында жедел жад дамптарын қалыптастыру мүмкіндігі;
* вирустық дерекқордың жаңартуларын алдыңғы нұсқаларға қайтару және көрсетілген уақыт аралығында жаңартуды автоматты түрде қосу арқылы олардың жаңартылуын тоқтата тұру мүмкіндігі;
* жаңарту кезінде вирус сигнатураларының деректер базасын және өнім модульдерін үзілген жүктеуді жаңарту функционалдығының болуы;
* Windows қауіпсіздік орталығымен интеграция;
* анықталған осалдықтарды жабатын патчтарды орнату үшін «міндетті емес» жаңартулардан «сыни» жаңартуларға дейін қажетті жаңартуларды таңдау арқылы Windows жаңарту орталығымен интеграция;
* орындалатын файлдарды және компьютердің жүктеу аймақтарын бөлек тапсырма ретінде тексеруді теңшеу;
* қосымшаның өзін-өзі қорғау, қосымша қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалардан, зиянкестерден немесе білікті емес пайдаланушылардан қорғауды өшірмеу үшін құпиясөз арқылы қосымшаның параметрлеріне кіруді қорғау технологиялары;
* жүйенің өзекті жаңартуларын тексеру;
* толық экран режимінде жұмыс істейтін қосымшалар үшін антивирустың жұмысы кезінде хабарландыруларды автоматты түрде жасырудың теңшелетін функциясының болуы, яғни қосымшаның толық экран режимінде жұмыс істеуі кезінде экранға вирусқа қарсы бағдарламалық жасақтаманың жұмысы туралы ақпараттық хабарламалар шығарылмайды;
* жұмыс стансаларында болып жатқан маңызды оқиғалар туралы әкімшілерге хабарлаудың көптеген жолдарының болуы (пошта хабарламасы, қалқымалы терезе, оқиғалар журналына жазу);
* байланыс арналары бойынша да, иеліктен шығарылатын ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен вирусқа қарсы базаларды жаңарту;
* логтар мен есептерді XML, TXT, DAT, DMP форматтарына экспорттау;
* белгісіз қауіптерді детектрлеудің бұлтты технологиясының болуы, беделді қызметке негізделген қосымшаларды бақылау;
* вирусты сарапшыларға зиянды код үлгілерін автоматты түрде немесе қолмен беру жүйесінің болуы
* авариялық қалпына келтіру дискілерін жасау мүмкіндігі;
* автономды қоректендіру режимінде электрэнергияны үнемдеу;
* вирусқа қарсы пакеттің дистрибутив көлемі 95 Мб аспауы керек.

**Microsoft Windows тобының ОЖ басқаруындағы серверлердің вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар** Microsoft Windows тобының ОЖ басқаруындағы серверлердің вирусқа қарсы қорғау бағдарламалық құралдары келесі OЖ нұсқаларында жұмыс істеуі керек:* Microsoft Windows Server 2003 (x86 и x64)
* Microsoft Windows Server 2003 R2 (x86 и x64)
* Microsoft Windows Server 2008 (x86 и x64)
* Microsoft Windows Server 2008 R2
* Microsoft Windows Server 2012
* Microsoft Windows Server 2012 R2

Серверы Storage, Small Business и MultiPoint:* Microsoft Windows Storage Server 2008 R2 Essentials спакетомобновления 1
* Microsoft Windows Storage Server 2012
* Microsoft Windows Storage Server 2012 R2
* Microsoft Windows Small Business Server 2003 (x86)
* Microsoft Windows Small Business Server 2003 R2 (x86)
* 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 тобының ОЖ басқаруындағы серверлердің вирусқа қарсы қорғау бағдарламалық құралдары келесі функционалдық мүмкіндіктерді жүзеге асыруды қамтамасыз етуі керек:* вирусқа қарсы бағдарламалық қамтамасыз ету интерфейсі сенсорлы экрандар мен жоғары ажыратымдылықты экрандарды қолдауды қамтамасыз етуі керек;
* резиденттік антивирустық мониторинг;
* пайдаланушы немесе әкімші пәрмені арқылы антивирустық сканерлеу;
* кесте бойынша антивирустық сканерлеу;
* белгілі бір жағдайларда антивирустық сканерлеу:
* - вирусқа қарсы дерекқорды жаңартқаннан кейін;
* - компьютерді әр іске қосу кезінде;
* - әр күн, компьютерді бірінші рет іске қосу кезінде;
* - табысты Интернет немесе VPN байланысы кезінде;
* - Пайдаланушының кіруі;
* - күдікті белсенділік анықталған кезде, соның ішінде «нақты уақыт режимінде қорғау» белсенді модулін қоса алғанда;
* трафикті келесі хаттамалар бойынша антивирустық сканерлеу: FTP, HTTP және HTTP, POP3 және POP3, сонымен қатар трафиктің IMAP және IMAPs;
* эвристикалық талдауға негізделген белгісіз зиянды бағдарламалардан қорғау;
* ДК-да орналасуына қарамастан, белгілі бір қауіптерге ерекше жағдайларды қосу мүмкіндігі:
* руткиттерді анықтау (жасырын файлдар / жүйелік ауытқулар);
* PKLITE, LZEXE, DIET, EXEPACK сияқты және т.б. бағдарламалармен жинақталған 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 форматтарындағы мұрағаттардағы файлдарды вирусқа қарсы тексеру және емдеу;
* тапсырмаларды кесте бойынша және / немесе операциялық жүйе жүктелгеннен кейін дереу іске қосу;
* антивирус жоспарлағышында үшінші тарап өндірушісінің қосымшасын іске қосу тапсырмасын жасау мүмкіндігі;
* Web-беттерден жүктелетін зиянды сценарийлерден жылдам қорғау;
* пәрмен жолының интерфейсінен вирусқа қарсы пакеттің параметрлерін теңшеу мүмкіндігі;
* үздіксіз жұмыс үшін сыни маңызы бар сервердегі файлдарды автоматты түрде анықтау және жою;
* сканерлеу жылдамдығын арттыру үшін сканерлеу модульдерінің санын беру мүмкіндігі;
* бұғатталған немесе рұқсат етілген веб-сайттардың тізімін жасау арқылы, сондай-ақ рұқсат етілген тізімге енгізілгендерден басқа барлық веб-сайттарға тыйым салу арқылы веб-ресурстарға қол жеткізуді басқару мүмкіндігі;
* қосымшалар үшін белсенді сүзгілеу режимі, сонымен қатар сүзгілеуді өшіру немесе шығарылған қосымшалар үшін пассивті режимге ауыстыру мүмкіндігі;
* контекстік мәзірден сканерлеу;
* сенімді веб-мекенжайлар үшін сүзгілеуді өшіру;
* көпағынды сканерлеу;
* Интернеттен жаңарту мүмкіндігі бар бірнеше жаңарту профильдерін (мысалы, мобильді пайдаланушылар үшін) теңшеу;
* вирусқа қарсы пакетте жоспарлаушының болуы;
* файлдық серверлер үшін вирусқа қарсы бағдарламалық жасақтаманы әкімшілендіру агентінің (AБЖ) болуы
* өзгерістерді бақылау және оларды уақыт аралығындағы суреттер арқылы автоматты түрде салыстыру мүмкіндігімен ДК жай-күйі туралы, орнатылған қосымшалар, қызметтер, желілік қосылымдар және т. б. туралы жалпы ақпаратты бір орталықтан көру мүмкіндігі, сондай-ақ жүйенің дұрыс жұмысын қалпына келтіретін өзгерістер (процестер мен драйверлерді тоқтату, тізілім жазбалары мен жүйелік файлдарды жою және қалпына келтіру) енгізу мүмкіндігі;
* ядро және барлық негізгі өнім модульдін қайта жүктеуді қажет етпейді және орнатудан кейін бірден белсенді болады;
* әкімшілендіру агентін орнату арқылы бұрыннан орнатылған жұмыс стансасының вирусқа қарсы қорғау лицензияларын орталықтандырылған басқару серверіне вирусқа қарсы қорғау пакетін жою қажеттілігінсіз қосу мүмкіндігі;
* белгісіз қауіптерді детекрлеудің бұлтты технологиясының болуы
* модем қосылымын немесе VPN орнатқаннан кейін вирусқа қарсы дерекқордың жаңартылуын іске қосу;
* жағдайы соңғы тексеру уақытынан бері өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету;
* вирусқа қарсы пакеті бар ықтимал проблемаларды шешуді тездету үшін антивирустық пакеттің конфигурациясы, орнату және жұмыс істеуі туралы журнал файлдарын жинауға арналған мамандандырылған утилитаның болуы;
* виртуалданған орталарда сканерлеу жылдамдығын арттыру үшін жалпы жергілікті кэшті пайдаланудың функционалдық мүмкіндігі;
* фишингтен қорғау: құпиясөздерді және басқа да құпия ақпаратты алу әрекеттерінен қорғайды, қалыпты веб-сайттар нысанын алатын зиянды веб-сайттарға кіруді болдырмайды;
* эксплойттардан қорғау: эксплойт-блокатор процестердің мінез-құлқын бақылайды және мақсатты шабуылдарға және бұрын белгісіз эксплойттар - нөлдік күннің қауіп-қатеріне тән күдікті әрекеттерді анықтайды;
* жадтағы бүркемені алып тастаған кезде процестердің әрекетін бақылайтын және зиянды процестерді сканерлейтін жадты сканерлеу модулінің болуы;
* жұмыстың басымдылығына байланысты антивирус пен басқа қосымшалар арасында жұмыс стансасының ресурстарын бөлуді реттеу: фондық режимде антивирустық сканерлеуді жалғастыру мүмкіндігі;
* параметрлер бойынша сканерлеу шектерін теңшеу – қабатталым тереңдігі (мұрағаттар), объектінің көлемі және объектінің сканерлеу уақыты;
* ауыстырылатын ақпарат және құрылғыларды (USB) бұғаттау;
* Windows қауіпсіздік орталығымен интеграция;
* анықталған осалдықтарды жабатын патчтарды орнату үшін «міндетті емес» жаңартулардан «сыни» жаңартуларға дейін қажетті жаңартуларды таңдау арқылы Windows жаңарту орталығымен интеграция;
* орындалатын файлдарды және компьютердің жүктеу аймақтарын бөлек тапсырма ретінде тексеруді теңшеу;
* қосымшаның өзін-өзі қорғау, қосымша қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалардан, зиянкестерден немесе білікті емес пайдаланушылардан қорғауды өшірмеу үшін құпиясөз арқылы қосымшаның параметрлеріне кіруді қорғау технологиялары;
* жүйенің өзекті жаңартуларын тексеру;
* графикалық интерфейссіз толық жұмыс, командалық жол арқылы АБЖ әкімшлендіру және конфигруациялау;
* АБЖ конфигурациялауға және кез-келген әрекетті орындауға мүмкіндік беретін сценарийлерді орындау арқылы жұмысты автоматтандыру мүмкіндігі;
* антивирустың толық экран режимінде жұмыс істеуі кезінде хабарландыруларды автоматты түрде жасыру;
* толық экран режимінде жұмыс істейтін қосымшалар үшін антивирустың жұмысы кезінде хабарландыруларды автоматты түрде жасырудың теңшелетін функциясының болуы;
* жұмыс стансаларында болып жатқан маңызды оқиғалар туралы әкімшілерге хабарлаудың көптеген жолдарының болуы (пошта хабарламасы, қалқымалы терезе, оқиғалар журналына жазу
* байланыс арналары бойынша да, иеліктен шығарылатын ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен вирусқа қарсы базаларды жаңарту;
* вирусты сарапшыларға зиянды код үлгілерін автоматты түрде немесе қолмен беру жүйесінің болуы
* авариялық қалпына келтіру дискілерін жасау мүмкіндігі
* вирусқа қарсы пакеттің дистрибутив көлемі 85 Мб аспауы керек

Вирусқа қарсы қорғауды басқару жүйесіне қойылатын талаптарБарлық қорғалатын ресурстарға арналған бағдарламалық басқару құралдары мынадай функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс:* ауқымды шешім;
* вирусқа қарсы бағдарлама интерфейсі сенсорлық экрандар мен жоғары ажыратымдылықты экрандарға қолдау көрсетуі керек;
* Прокси-сервер - шешімнің жоғары ауқымдылығын қамтамасыз ететін және орталық әкімшілендіру серверіне жүктемені азайтатын компонент;
* жергілікті желіде ДК автоматты түрде іздейтін белгісіз компьютерлерді қолмен іздеуді және қосуды қажет етпестен табуға арналған құралдың болуы;
* вирусқа қарсы бағдарламалық құралдарды, теңшелімді, әкімшілендіруді орталықтандырылған орнату / жаңарту / жою;
* ақпаратты орталықтандырылған жинау және вирусқа қарсы қорғау жағайды туралы есептер жасау;
* сервер мен клиент арасындағы сенімді байланыс;
* басқарудың орталықтандырылған бағдарламалық құралдарында есептерді басқару және жасау үшін WEB консолы болуы керек;
* орталықтандырылған басқару кез келген құрылғыдан Web -браузер арқылы орындалуы мүмкін;
* есептерді көрнекті графикалық түрде жасау;
* логтар мен есептерді HTML, TXT, CSV, PDF форматтарына экспорттау;
* SIEM қолдау модулінің болуы;
* топтар немесе клиенттер үшін саясаттарды алдын ала теңшеу (жаңарту профильдері, тыйым салынған сайттар, жоспарлаушы кестесі және т.б.);
* мобильді құрылғыларға да, дербес компьютерлерге де хабарлама жіберу мүмкіндігі;
* мобильді құрылғыдан қашықтан қауіпсіздік аудит журналын жасау мүмкіндігі
* Пайдаланушылық қосымшаларды орнату мүмкіндігі;
* антивирустық бағдарламалық қамтамасыз етудің клиенттік бөлігінің әкімшілендіру агенттерін орнатудың әр түрлі нұсқаларының болуы:

қашықтан немесе жергілікті:- Push орнату;- e-mail арқылы орнату;- алынбалы тасымалдаушыны пайдалана отырып орнату, мысалы USB;- Жергілікті орнату;* операциялық жүйелер үшін немесе қол режимінде агенттің тиісті орнату пакетін автоматты түрде таңдау мүмкіндігі
* клиенттер үшін қауіпсіздік саясатын теңшеу;
* өзгерістерді бақылау және оларды уақыт аралығындағы суреттер арқылы автоматты түрде салыстыру мүмкіндігімен ДК жай-күйі туралы, орнатылған қосымшалар, қызметтер, желілік қосылымдар және т. б. туралы жалпы ақпаратты бір орталықтан көру мүмкіндігі, сондай-ақ жүйенің дұрыс жұмысын қалпына келтіретін өзгерістер (процестер мен драйверлерді тоқтату, тізілім жазбалары мен жүйелік файлдарды жою және қалпына келтіру) енгізу мүмкіндігі;
* жүйенің маңызды объектілерін жоюға/өзгертуге арналған соңғы клиенттерде белгілі бір сценарийді қашықтан іске қосу мүмкіндігі;
* вирусқа қарсы қорғауды басқару жүйесін орнатқаннан кейін компьютерді қайта жүктеудің қажеті жоқ;
* вирусқа қарсы бағдарламалық құралдарды және вирусқа қарсы дерекқорларды автоматтандырылған жаңарту;
* дербес компьютерлер немесе топтар үшін сигнатура базаларының жаңартуларын жылдам қайтару мүмкіндігі
* пайдаланушылар жұмыс стансаларына жаңартуларды қабылдаудан кейін бірден жеткізу;
* орталықтандырылған карантин;
* Басқарылатын компьютерлер тобын қолмен немесе автоматты түрде Active Directory құрылымының негізінде құру;
* Active Directory-мен кестеде бойынша да, қолмен де синхрондау мүмкіндігі;
* желі топологиясын ескере отырып қорғалмаған жұмыс стансаларын автоматты іздеу;
* Есептік жазбалар бойынша сервер теңшеліміндегі өзгерістер аудиті;
* қорғау модульдерін белгілі бір уақыт аралығында немесе компьютерді қайта іске қоспас бұрын өшіру мүмкіндігі;
* әкімшілердің және операторлардың рөлдерін, сондай-ақ әр деңгейде ұсынылатын есептердің нысандарын теңшеу мүмкіндігі бар көп деңгейлі басқару жүйесін құру;
* әр түрлі көздерден бағдарламалық қамтамасыз етуді және вирусқа қарсы базаларды байланыс арналары арқылы да ақпараттық тасымалдаушылар арқылы да жаңарту;
* вирусқа қарсы қосымшаларды қолданудағы оқиғалар туралы хабардар ету механизмі және олар туралы пошта хабарландыруларын таратуды теңшеу мүмкіндігі;
* вирус сарапшыларына зиянды код үлгілерін автоматты түрде немесе қолмен беру жүйесінің болуы;
* осы топтардың шарттарына сәйкес келсе клиенттік станциялар динамикалық түрде қосылатын динамикалық топтарды құру мүмкіндігі;
* статикалық және динамикалық топтармен жұмыс істеу;
* желі әкімшісін хабарландырудың әр түрлі нұсқалары (email арқылы, SNMP тұзақтарын пайдалану);
* деректер базасы мазмұнының және сервер теңшелімдерінің резервтік көшірмелерін жасау мүмкіндігі;
* қашықтағы әкімшілік серверінің консоліне домен пайдаланушысының аты мен құпиясөзін пайдаланып қосылу мүмкіндігі;
* Windows, Linux \ BSD серверлері мен жұмыс стансаларын, сондай-ақ мобильді ОЖ (Android) қорғауға арналған шешімдерін әкімшілендіру;
* Wakeon LAN жергілікті желісі бойынша ояту функциясының болуы
* әкімшілендіру сервермен деректер алмастыруды үзу немесе жаңарту үшін таңдалған компьютерлерде хабарландыруларды тез ажырату немесе қосу функциясының болуы
* MS SQL MySQL дерекқорларын, қолдау;
* орталықтандырылған басқару бағдарламалық құралдарын Windows және Linux платформаларында орнатуға болады
* бағдарламалық құралдар Windows және Linux платформаларының бұзылысқа төзімді кластерлеріне орнатуды қолдауы керек
* қашықтан басқару серверін орнатуға болады және Windows Server операциялық жүйелерге қолдау көрсетуі тиіс

Windows Server:* + Windows Server 2003 x86 SP2 /x64 SP2
	+ Windows Server 2003 x86 R2 SP2 /x64 R2 SP2
	+ Windows Server 2008 x64 R2 SP1 / x64 R2 CORE
	+ Windows Server 2008 x86 SP2 / x64 SP2
	+ Windows Server 2012 x64 / x64 CORE
	+ Windows Server 2012 x64 R2 / x64 R2 CORE
	+ Microsoft SBS 2003 x86 SP2 / x86 R2
	+ Microsoft SBS 2008 x64 SP2
	+ Microsoft SBS 2011 x64 Standard / x64 Essential

Linux:* + Ubuntu 12.04 LTS x86 Desktop / Server
	+ Ubuntu 12.04 LTS x64 Desktop / Server
	+ Ubuntu14.04. LTS x86 Desktop / Server
	+ Ubuntu 14.04 LTS x64 Desktop / Server
	+ RHEL Server 6 x86 / x64
	+ RHEL Server 7 x86 / x64
	+ CentOS 6 x86 / x64
	+ CentOS 7 x86 / x64
	+ SLED 11 x86 / x64
	+ SLES 11 x86 /x64
	+ OpenSUSE 13 x86 / x64
	+ Debian 7 x86 / x64
	+ Fedora 19 x86 / x64
* Лицензияларды басқару үшін арнайы бағдарламалық құралдың болуы. Оның көмегімен лицензияларды, белсендірілген модульдерді және қолданылу мерзімінің аяқталуы, пайдалану және авторизация сияқты лицензиялармен байланысты оқиғаларды бақылауға болады. Лицензия иесі немесе қауіпсіздік әкімшісі ретінде әр түрлі рөлдерде құралмен жұмыс істеу.

Келесі әрекеттерді орындау мүмкіндігі:* Шынайы уақытта лицензиялардың жай-күйін қарау;
* жеке құрылғыларды бақылау (және сонымен бірге оларды өшіру);
* лицензия оқиғаларына қатысты хабарландыруларды теңшеу;
* бір мезгілде аралас орталарда ескі және жаңа пішіндерде лицензияларды сақтау;
* бағдарламаларды іске қосуға болатын электрондық пошта хабарламалары мен құпиясөздерге лицензия кілттерін ауыстыру;
* бір есептік жазбаға бірнеше лицензияны тағайындау;
* басқа тұлғаларға лицензияны пайдалануға рұқсат ету (оларды белсендіру);
* лицензияның жай-күйін ыңғайлы қадағалау үшін хабарландыруларды теңшеу;
* орталықтандырылған басқару серверімен синхрондау функциясының болуы.

**Вирусқа қарсы базаларды жаңартуға қойылатын талаптар**Жаңартылатын вирусқа қарсы базалар келесі функцияларды қамтамасыз етуі керек:* трафикті үнемдеу үшін айна жаңартуларын жасау мүмкіндігі жүзеге асырылды;
* жаңарту айнасын Windows/Linux операциялық жүйесіне қарамастан, кез-келген желідегі компьютерде, соның ішінде AV клиентін қолдана отырып, соңғы жұмыс станциясында кем дегенде екі жаңарту жолының (HTTP және SMB) міндетті түрде қатысуымен жасауға болады, айнаны іске қосу үшін сервер сияқты да, жұмыс стансасы сияқты да қосымша модульдерді орнату талап етілмейді;
* жаңартулар түрлері: вирус сигнатураларының ДҚ, бағдарламалық компоненттерін жаңарту, ядроны жаңарту;
* айнаны жаңарту пакеттерін екі жолмен жүктеуге болады: HTTP протоколы бойынша (ұсынылады) және ортақ желілік диск (SMB) көмегімен;
* жаңартуларды электрондық ақпарат тасығыштарда (FDD\CD\ DVD\USB-drive) таратуға болады;
* электрондық цифрлық қолтаңба құралдары арқылы жаңартулардың тұтастығы мен түпнұсқалығын тексеру жүзеге асырылады.

**Әлеуетті өнім берушіге қойылатын талаптар**Әлеуетті өнім беруші лицензиялық бағдарламалық қамтамасыз етуді өндірушіден авторизациялау хатын ұсынуы тиіс Лицензияның қолданылу мерзімі 2023 жылғы желтоқсанда аяқталуы тиіс.**Лицензиялық келісімде мынадай деректер көрсетілуі тиіс:**Өнімнің атауы, қорғалатын объектілердің саны, лицензияның аяқталу күні, сериялық нөмірі және осы лицензияның құқық иеленуші ұйымының атауы. |
| 4. | Орындаушы жеңімпаз деп анықталған жағдайда әлеуетті өнім берушіге қойылатын талаптар және онымен мемлекеттік сатып алу туралы шарт жасасу (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені немесе бермегені үшін қабылдамауға жол берілмейді) |  |