2000 дербес компьютер мен серверлік жабдықтың антивирустық қорғанысын орталықтандырылған басқаруға қойылатын өнім талаптары

Жалпы талаптар

1. Бағдарламалық өнімдердің интерфейсі, соның ішінде орталықтандырылған басқару құралдары ағылшын және орыс тілдерінде болуы тиіс.
2. Бағдарламалық өнімдерде, соның ішінде орталықтандырылған басқару құралдарында ағылшын және орыс тілдеріндегі контекстік анықтамалық жүйе болуы тиіс.
3. Бағдарламалық өнім үшін, соның ішінде орталықтандырылған басқару құралдары үшін мемлекеттік стандарттардың талаптарына сәйкес дайындалған, ағылшын және орыс тілдеріндегі пайдалану құжаттамасының, соның ішінде «Пайдаланушы (әкімші) нұсқаулығының» болуы.
4. Бағдарламалық өніммен, соның ішінде орталықтандырылған басқару құралдарымен бірге жеткізілетін құжаттама тиісті бағдарламалық өнімді орнату, баптау және пайдалану процесін егжей-тегжейлі сипаттауы тиіс.
5. Бағдарламалық өнімге, соның ішінде орталықтандырылған басқару құралдарына техникалық қолдау көрсету орыс және ағылшын тілдерінде бағдарламалық өнімді өндірушінің сертификатталған мамандарымен телефон, электрондық пошта арқылы және қажет болған жағдайда тапсырыс берушіге жедел бару арқылы көрсетілуі тиіс.
6. Бағдарламалық шешімді өндірушінің веб-сайты ағылшын және орыс тілдерінде болуы, сондай-ақ бағдарламалық өнімді техникалық қолдауға арналған арнайы бөлімі, өзекті білім базасы және бағдарламалық өнімдерді пайдаланушылардың форумы болуы тиіс.

Консоль (Басқару сервері)

1. Бірыңғай веб-интерфейстен бүкіл желілік инфрақұрылымның антивирустық қорғанысын орталықтандырылған басқару мүмкіндігі.
2. Бас сервер мен бағынышты серверлерден тұратын әкімшілендірудің иерархиялық құрылымын құру мүмкіндігі, бұл бас бөлімшеге де, өңірлік бөлімшелерге де тиесілі жұмыс станцияларының, серверлердің және мобильді құрылғылардың антивирустық қорғанысын орталықтандырылған басқаруды жүзеге асыруға мүмкіндік береді.
3. Windows, macOS және Linux басқаруындағы соңғы құрылғылар мен серверлерде орнатылған жабдықтарды түгендеу (инвентаризациялау).
4. Windows, macOS және Linux басқаруындағы жұмыс станциялары мен серверлерде орнатылған бағдарламалық жасақтаманы түгендеу (инвентаризациялау).
5. Windows, Linux және macOS операциялық жүйелеріне арналған әртүрлі пайдаланушылық бағдарламалық жасақтаманы да, антивирустық бағдарламалық жасақтаманы да бір уақытта бірнеше соңғы нүктелерге қашықтан орнату құралының болуы.
6. Windows, Linux және macOS операциялық жүйелері үшін пайдаланушылық бағдарламалық жасақтаманы да, антивирустық бағдарламалық жасақтаманы да қашықтан жою (деинсталляциялау) функциясының болуы.
7. Қашықтан басқару құралының көмегімен қосымша желілік әрекеттерді орындау мүмкіндігі, мысалы: жұмысты аяқтау және қайта жүктеу, компьютерді ояту сигналын (wake-on-LAN) жіберу, хабарламалар жіберу, клиенттік компьютерде

нақты командалық жол нұсқауларын орындау, клиенттік компьютердің операциялық жүйесін жаңартуды бастау.

8. Конфигурация параметрлері алдын ала орнатылған Windows, Linux және macOS операциялық жүйелеріне арналған орнату пакеттерін жасау және өңдеу құралының болуы, бұл оқшауланған желідегі соңғы нүктелерде, сондай-ақ қорғауды қажет ететін, бірақ әкімшілендіру серверіне уақытша қосылмаған соңғы нүктелерде толыққанды антивирустық қорғанысты өрістету үшін орнату пакеттерін экспорттауға мүмкіндік береді.
9. Әкімшілендіру серверінің пайдаланушыларын құруға және оларға жеке бөлімдерге, әкімшілендіру серверіндегі компьютерлер топтарына әртүрлі қолжетімділік құқықтарын тағайындауға мүмкіндік беретін пайдаланушылар диспетчерінің болуы, бұл антивирустық қорғаныстың тармақталған жүйесінің өңірлік жүйелік әкімшілері үшін әртүрлі қолжетімділік құқықтарын беруге мүмкіндік береді.
10. Active Directory қауіпсіздік топтарының көмегімен басқару консолінің әкімшілерін аутентификациялау мүмкіндігі.
11. Әкімшілердің тіркелгілері үшін екі факторлы аутентификацияны пайдалану мүмкіндігі, бұл орталықтандырылған басқару серверіне рұқсатсыз қосылудың алдын алуға мүмкіндік береді.
12. Конфигурациядағы барлық өзгерістер мен әкімшілендіру серверінің пайдаланушылары орындайтын барлық әрекеттер тіркелетін және қадағаланатын аудит журналының болуы.
13. Жеке алынған клиентте дербес брандмауэр, нақты уақыт режиміндегі қорғаныс, пошта клиентін қорғау, Интернетке қол жеткізуді қорғау, құрылғыларды бақылау, веб-бақылау, антиспам сияқты қорғаныс модульдерін қашықтан белсендіру және белсенділігін жою мүмкіндігі.
14. Статикалық топтарды жасау және өңдеу мүмкіндігі және Active Directory жүйесінен компьютерлер тармағын импорттау мүмкіндігі.
15. Клиенттерді көптеген критерийлер бойынша динамикалық топтарға автоматты түрде бөлуді баптау, соңынан тиісті қауіпсіздік саясаттарын тағайындау, сондай-ақ қажетті тапсырмаларды іске қосу мүмкіндігі.
16. Құрылғыларды бақылау және веб-бақылау ережелерін дербестендіру үшін пайдаланушылар мен топтарды Active Directory жүйесінен кейіннен пайдалану үшін импорттау мүмкіндігі.
17. Антивирустық өнімдердің конфигурациялық параметрлеріне тұрақты қызмет көрсетуге арналған кірістірілген және пайдаланушылық саясаттарды пайдалану мүмкіндігі. Саясаттарды экспорттауды/импорттауды жүзеге асыру мүмкіндігі.
18. Инфрақұрылымның қауіпсіздігін қорғау деңгейіне, қорғалған соңғы нүктелердің күйіне, сондай-ақ әкімшілендіру серверінің өзінің күйіне қатысты барлық қажетті егжей-тегжейлі ақпаратты ұсынатын мониторинг панелінің болуы.
19. Мониторинг панелі үшін де, әртүрлі есептерді қалыптастыру үшін де пайдаланылуы мүмкін кемінде 100 алдын ала орнатылған есеп үлгілерінің болуы.
20. Мониторинг панелі үшін де, PDF, CSV форматтарында есептерді қалыптастыру және көрсетілген жол бойынша кейіннен сақтау немесе көрсетілген электрондық поштаға жіберу үшін пайдаланылатын есеп үлгілерін жасау және өңдеу мүмкіндігі.
21. Microsoft Sentinel, Stellar Cyber, IBM QRadar, Wazuh, Elastic немесе Splunk сияқты жетекші SIEM жүйелерімен интеграцияны қолдау.
22. Сұрауларды жіберу және тиісті қауіпсіздік оқиғалары мен телеметрияны тікелей алу үшін сыртқы SIEM жүйелеріне REST API ұсыну мүмкіндігінің болуы.

23. SIEM жүйесімен кейіннен интеграциялау үшін журналдарды syslog-қа экспорттау мүмкіндігі.
24. Журналдар мен есептердің параметрлерін баптау немесе әртүрлі жүйелер/клиенттер үшін 50-ден астам үлгілердің ішінен таңдау мүмкіндігі.
25. Антивирустық өнімнің, арнайы утилитаның немесе прокси-сервердің көмегімен

жаңартулар айнасын (зеркало обновлений) жасау мүмкіндігі.
26. Сыртқы HTTP-серверлер негізінде жаңартулар айнасын жасау мүмкіндігі.
27. Сертификатпен қорғалған қосылым арқылы кез келген браузер арқылы серверді басқаруға мүмкіндік беретін веб-бағытталған интерфейс.
28. Соңғы нүктелердегі антивирустық өнімді қашықтан басқаруға, сондай-ақ жұмыс станцияларындағы антивирустық қорғаныс деңгейін және операциялық жүйенің күйін бақылауға мүмкіндік беретін тәуелсіз агентті пайдалану.
29. Басқару агентінің модулі келесі талаптарға сай болуы тиіс:
− жеңілдетілген ядро түрінде таратылуы (алдын ала орнатылған функционалдық модульдерсіз);
− белсендірілген саясаттар мен қосылған қорғаныс функциялары негізінде басқару серверінен функционалдық модульдерді жүктеуді қолдауы;
− басқару серверімен деректер алмасудың екі жақты режимін қамтамасыз етуі;
− командалық жолдан басқаруды қолдауы;

29. Жұмыс станциясында орнатылған бағдарламалық жасақтаманы (БЖ) қадағалау және оның күйін басқару, сондай-ақ таңдау бойынша орнатылған БЖ жою мүмкіндігі.
30. Мобильді құрылғылардағы антивирустық қорғанысты басқаруға мүмкіндік беретін қосымша компоненттің болуы.
31. Оларға кейіннен антивирустық қорғанысты өрістету үшін желідегі қорғалмаған жұмыс станцияларын анықтауды жүзеге асыратын арнайы компонент.
32. Сервер компоненттері арасындағы қосылымдарды дербес шығарылған сертификаттардың да, қолданыстағы сертификаттардың да көмегімен қорғау.
33. Ransomware Shield қолданыстағы функциясын толықтыратын және шифрлау процесі басталғаннан кейін, шабуылдың соңғы кезеңдерінде бопсалаушы бағдарламалар (ransomware) анықталған кезде шифрланған файлдарды автоматты түрде қалпына келтіру функциясы бар патенттелген технологияның болуы.
34. Лицензиялардың күйін басқаруға арналған құрал (тіпті әкімшілендіру серверін пайдаланбай-ақ).
35. Физкалық немесе қашықтан қол жеткізу мүмкіндігі жоқ жұмыс станцияларында да антивирустық өнімдердің лицензиясын белсенділігін жою (деактивировать) мүмкіндігі.

37. VDI жүйелерінде көшіру немесе клондау үшін қандай виртуалды машина дереккөз болатынын анықтау мүмкіндігі.
38. VDI жүйелерімен интеграциялау үшін егжей-тегжейлі параметрлерді анықтауға арналған баптау шеберінің (мастер настройки) болуы.
39. Клондалған компьютерлердің идентификаторларын өңдеу нұсқаларын таңдау мүмкіндігі, мысалы, қолданыстағы компьютерлермен сәйкестендіру немесе жаңа компьютерлер құру.
40. Лездік клондар (мгновенные клоны) немесе машиналар каталогтары үшін VDI атау беру үлгісінің (шаблон именования VDI) параметрлерін анықтау мүмкіндігі.
41. VDI жүйелерімен интеграцияның дұрыс бапталмағаны туралы хабардар етуге мүмкіндік беретін, клондалған машиналардың қате сәйкестендірілуі (идентификациялануы) туралы хабарлау үшін хабарландыру жүйесінде алдын ала орнатылған үлгілердің болуы.
42. Әкімшілердің араласуынсыз өзекті нұсқаларды пайдалануға мүмкіндік беретін басқару агентін автоматты түрде жаңарту функциясының болуы.
43. Желіге және жалпы компьютерлерге түсетін жүктемені азайтуға мүмкіндік беретін автоматты жаңарту процесін бөлу (распределение) механизмінің болуы.
44. Басқару агентін ARM64 процессорларына орнату мүмкіндігі.
45. Лицензияның белгілі бір бөлігін жекелеген филиалдарға тағайындауға мүмкіндік беретін компанияның филиалдарына сәйкес алаңдарды (площадкаларды) құру функциясының болуы.

46. Тиісті лицензия бөлігі бар алаң немесе филиал әкімшісін анықтауға арналған функционалдың болуы.
47. Басқару агенті қолдайтын ОЖ (операциялық жүйелер): Microsoft Windows 10 / 11; Red Hat Enterprise Linux (RHEL) 8 / 9; CentOS 7.9; Ubuntu Desktop 20.04 LTS / 22.04 LTS / 24.04 LTS; Debian 11 / 12; SUSE Linux Enterprise Server (SLES) 15; Oracle Linux 8 / 9; Amazon Linux 2 / 2023; Alma Linux 8 / 9; Rocky Linux 8 / 9; Linux Mint 20 / 21 / 22; macOS 11 / 12 / 13 14 / 15 / 26.

Жұмыс станцияларын қорғау

1. Вирустардан, трояндық БЖ-дан, жарнамалық БЖ-дан, фишингтен, сондай-ақ шпиондық БЖ-дан қорғанысты қамтамасыз ету.
2. Зиянды БЖ-дан – компьютердегі файлдар кодының басына немесе соңына қосылатын белгілі бір зиянды кодтан қорғанысты қамтамасыз ету. Зиянды БЖ-ны анықтауды машиналық оқыту компонентімен ұштастырылған анықтау ядросы жүзеге асыруы тиіс.
3. Вирустар немесе трояндар сияқты сөзсіз зиянды бағдарламаларға ұқсас, зиянды БЖ-ға бірмәнді жатқызуға болмайтын, бірақ қосымша қажетсіз БЖ орната алатын, жүйе параметрлерін өзгерте алатын, сондай-ақ күтілмеген әрекеттерді немесе пайдаланушы растамаған әрекеттерді орындай алатын әлеуетті қажетсіз бағдарламалардан қорғанысты қамтамасыз ету.
4. Әлеуетті қауіпті бағдарламалардан – рұқсатсыз қашықтан қол жеткізу, құпия сөздерді ұрлау немесе бұзу, пернетақта тыңшылары (кейлоггерлер) және басқалары сияқты зиянды мақсаттарда пайдаланылуы мүмкін әртүрлі БЖ-дан қорғанысты қамтамасыз ету.
5. Күдікті бағдарламалардан – қаскүнемдер зиянды бағдарламалық жасақтаманың анықталуын болдырмау үшін жиі пайдаланатын, буып-түйгіштермен (упаковщики) немесе қорғағыштармен (протекторы) қысылған бағдарламалардан қорғанысты қамтамасыз ету.

6. Интернеттегі қаскүнемдерге операциялық жүйеде өздерінің бар екендігін жасыра отырып, жүйеге шектеусіз қол жеткізуді қамтамасыз ететін руткиттер сияқты қауіпті бағдарламалардан қорғанысты қамтамасыз ету.
7. Қауіп-қатерлердің әртүрлі санаттары үшін қорғаныс үшін де, есептілік үшін де әрекет етудің (реагирования) жеке деңгейлерін баптау мүмкіндігі.
8. Зиянды емес, бірақ сканерлеу жұмысында ауытқуларға әкеп соғуы немесе жүйенің өнімділігіне әсер етуі мүмкін белгілі бір файлдарды сканерлеуден алып тастау (ерекшеліктер жасау) мүмкіндігі.
9. Жүйелік қызметтердің жұмыс жылдамдығын арттыру және ОЖ жұмыс процесіне араласуды барынша азайту мақсатында жалпыжүйелік процестер үшін ерекшеліктер жасау мүмкіндігі.
10. Жүктеу секторларын, соның ішінде UEFI интерфейсін, негізгі жүктеу жазбасында (MBR) вирустардың бар-жоғына тексеруді жүзеге асыру мүмкіндігі.

11. Нақты уақыт режимінде антивирустық қорғанысты қамтамасыз ету.
12. Сканерлеу кезінде өзіндік әзірлемедегі эвристикалық технологияларды пайдалану.
13. Пайдаланушының немесе әкімшінің талабы бойынша және кестеге сәйкес антивирустық сканерлеу құралының болуы.
14. Microsoft Office макростарын зиянды кодтың бар-жоғына тексеруге мүмкіндік беретін құжаттарды қорғау модулі.
15. ОЖ іске қосылуы кезінде файлдарды сканерлеу мүмкіндігі.
16. WMI және жүйелік реестрді, барлық бөлімдер мен бөлімшелерді сканерлеу мүмкіндігі, бұл деректер түрінде таралатын зиянды бағдарламалық кодтан және қаскүнемдік сілтемелерден қорғауды қамтамасыз етеді.
17. Conficker, Sirefef, Necurs және басқалары сияқты күрделі тұрақты қауіптердің қалдықтарын тазартуға арналған бірнеше утилиталарды біріктіретін кірістірілген құралдың болуы.
18. Компьютерді белсенді емес (белсенді емес уақытта/idle state) күйде сканерлеу.
19. Антивирустық сканер жұмысының егжей-тегжейлі параметрлерін анықтау мүмкіндігі, мысалы, сканерлеу объектілері мен әдістерін анықтау, файлды сканерлеудің максималды өлшемі мен уақытын белгілеу мүмкіндігі, архивтің максималды ішкі салыну тереңдігі және ерекшеліктер жасау.
20. Жүйеге түсетін жүктемені азайтатын және ең жылдам әрі тиімді сканерлеуді жүргізуге мүмкіндік беретін сканерлеу үшін кемінде 64 биттік ядроны пайдалану.
21. Зиянды әрекеттер мен зиянды бағдарламалық жасақтаманың сипаттамаларын анықтау мақсатында кодты тереңірек талдау үшін машиналық оқыту технологияларын пайдалану мүмкіндігі.
22. Java, Flash және басқалары сияқты әртүрлі қосымшалардың осалдықтарын пайдалана алатын қауіп-қатерлерден қорғауды қамтамасыз ететін эксплойттардан қорғау модулі.
23. Іске қосылған процестерді және олардың файлдық жүйедегі қызметін терең талдауға қабілетті, бопсалаушы бағдарламалардан (ransomware) қорғаудың қосымша деңгейін қамтамасыз ететін модульдің болуы.
24. Күдікті іске қосылған процестердің жұмысын қадағалауға қабілетті жедел жадты сканерлеу модулінің болуы, бұл тіпті мұқият шифрланған және жасырын қауіптердің жұқпалы әсерін болдырмауға мүмкіндік береді.
25. Бағдарламалардың іске қосылуын және жүйелік реестрдегі өзгерістерді қадағалайтын және компьютерді зиянды бағдарламалардан және қажетсіз белсенділіктен қорғайтын басып кіруді анықтау жүйесінің (HIPS) болуы.

26. Іске қосылған процестерді, орындалатын файлдарды және реестр бөлімдерін бақылау үшін жеке ережелерді жасау мүмкіндігі.
27. Іске қосылған процестерді бұлттық бедел қызметінде (облачный репутационный сервис) қосымша тексеру функциясының болуы.
28. Қосымша бағдарламалық өнімдерді орнату қажеттілігінсіз жұмыс станциялары мен серверлерді қорғауды бұлттық құмсалғышпен (қосымша

лицензия болған жағдайда) интеграциялау мүмкіндігі.
29. Ауысымдық ақпарат тасымалдағыштарды автоматты түрде антивирустық тексеру функциясының болуы.
30. Қол жеткізу ережелерін, атап айтқанда: бұғаттау, рұқсат ету, тек оқу, оқу және жазу, ескерту жасау арқылы жұмыс станциясына ауысымдық ақпарат тасымалдағыштардың қосылуын бақылауды жүзеге асыра алатын құралдың болуы.
31. Жұмыс станциясына сыртқы құрылғылардың қосылуын түрі бойынша, өндірушісі, моделі немесе құрылғының сериялық нөмірі бойынша бақылауды жүзеге асыру мүмкіндігі.
32. Рұқсат етілген немесе тыйым салынған сыртқы құрылғылардың топтарын жасау мүмкіндігі.
33. Сыртқы құрылғылардың қосылуына барлық пайдаланушылар үшін де, Windows немесе доменнің жекелеген пайдаланушылары немесе топтары үшін де тыйым салу немесе рұқсат ету мүмкіндігі.
34. Құрылғыларды бақылау ережелерін икемді баптауға мүмкіндік беретін уақыт аралықтарын (интервалдарын) белгілеу мүмкіндігі.
35. Бағдарламалық өнім POP3, POP3S, SMTP, IMAP және IMAPS хаттамаларын тексеру және пошталық тіркемелерді тексеру мүмкіндігімен пошта клиентіне интеграциялану арқылы жұмыс станциясындағы пошта трафигін қорғаудың қосымша деңгейін қамтамасыз етуі тиіс, әсіресе корпоративтік желіден тыс жерде уақытша немесе тұрақты болатын соңғы құрылғыларда.
36. Зақымдалған поштаны автоматты түрде жою немесе пошта клиентіндегі көрсетілген каталогқа ауыстыру мүмкіндігінің болуы.
37. Әсіресе корпоративтік желіден тыс жерде уақытша немесе тұрақты болатын соңғы құрылғыларда спамнан қорғаудың қосымша деңгейін қамтамасыз ететін, пошта клиентіне интеграциялану мүмкіндігі бар өзіндік әзірлемедегі спамнан қорғау модулінің болуы.
38. Спам-адресаттардың ақ және қара тізімдерін пайдаланушылық (интеллектуалды спам-модульді икемді дербестендіру) ретінде де, жаңарту серверлерінен келетін жаһандық тізімдер ретінде да пайдалану мүмкіндігі.
39. HTTP, HTTPS трафигін тексеру арқылы Интернет-трафикті қорғаудың қосымша деңгейін қамтамасыз ету мүмкіндігінің болуы, бұл осы хаттамалармен берілетін файлдарды бұғаттап қана қоймай, сонымен қатар фишингтік сайттар, ботнеттер серверлері, APT командалық (C&C) серверлері, сондай-ақ «ransomware» класындағы қауіптерді тарататын серверлер сияқты қауіпті ресурстардың мекенжайларын бұғаттауға мүмкіндік береді.
40. Бұғатталған, рұқсат етілген немесе тексеруден алып тасталған URL-мекенжайлардың тізімдерін жасау мүмкіндігі.
41. Әсіресе корпоративтік желіден тыс жерде уақытша немесе тұрақты болатын соңғы құрылғыларда Интернеттен файлдарды көрсетілген кеңейтілімі бойынша жүктеуді бұғаттау мүмкіндігі.
42. SSL хаттамасын автоматты және интерактивті режимдерде тексеру мүмкіндігі.

43. SSL-трафик сертификаттарының жарамдылығы мен тұтастығын тексеру мүмкіндігі.

44. Сенімді сертификаттар мен тексеруден алып тасталған сертификаттар тізімдерін басқару мүмкіндігі, сондай-ақ сертификат жарамсыз, белгісіз немесе зақымдалған деп анықталған кезде әрекетті таңдау мүмкіндігі.
45. Браузердің жады аймағына және оның терезелерінің мазмұнына араласу әрекеттерін бұғаттау мақсатында браузерлерді қорғалған режимде іске қосуға мүмкіндік беретін, сондай-ақ Интернет-төлемдер мен Интернет-банкинг және т.б. сияқты маңызды Интернет-қосылымдарды қосымша қорғауды қамтамасыз ететін қосымша модульдің болуы.
46. Жекелеген бағдарламалар мен жекелеген IP-объектілер (IP-мекенжайлар, IP-мекенжайлар ауқымы, ішкі желілер) үшін трафикті тексеру бойынша ерекшеліктер жасау мүмкіндігі.
47. Сыртқы және жергілікті желілік шабуылдардан желілік сүзгілеуді және қорғауды жүзеге асыруға арналған дербес брандмауэрдің болуы.

48. Дербес брандмауэрде жаңа белгісіз желілік қосылым туралы егжей-тегжейлі ақпаратты ұсынатын және ДК-де анықталған қосылым үшін жаңа желілік сүзгілеу ережесін жасап қана қоймай, ол үшін егжей-тегжейлі баптауларды көрсетуге мүмкіндік беретін интерактивті режимнің болуы.
49. Дербес брандмауэрде әкімшіге желілік қосымшалар мен жабдықтар үшін рұқсат етуші ережелерді қашықтан баптауға мүмкіндік беретін оқыту режимінің болуы.
50. Жаңадан жасалған ережелерді өңдеп қана қоймай, рұқсатсыз желілік қосылымдардан және жергілікті желілік шабуылдардан алғашқы мұқият қорғау үшін жеткілікті болып табылатын кірістірілген ережелерді басқаруға мүмкіндік беретін ережелер редакторының болуы.
51. Нақты бағдарламалар мен сервистер үшін желілік сүзгілеу ережелерін жасау мүмкіндігі.
52. Компьютердің қандай желіге қосылғанына байланысты автоматты түрде ауыса алатын дербес брандмауэр үшін әртүрлі профильдерді жасау мүмкіндігі.
53. ДК-нің белгісіз қауіпті желілерге рұқсатсыз қосылуының алдын алу мақсатында дербес брандмауэрде қосымша желілік аутентификацияны пайдалану мүмкіндігі.
54. Дербес брандмауэрде барлық желілік қосылымдар бойынша бүкіл егжей-тегжейлі ақпаратты қарауға, сондай-ақ пайдаланушыға қорғалмаған Wi-Fi желісіне қосылғаны туралы ескертуге мүмкіндік беретін қосымша функционалдың болуы.

55. Компьютерге жасалуы мүмкін желілік шабуылдардың әртүрлі түрлерін анықтау мақсатында басып кіруді анықтау жүйесі (IDS) модулінің қосымша параметрлерін баптау мүмкіндігі.
56. «Ботнет» типті қауіп-қатерлерден қорғанысты қамтамасыз ететін технологияның болуы.
57. Желілік хаттамалардың осалдықтарын қорғау, бұл SMB, RPC, RDP және басқалары сияқты желілік хаттамалардың кемшіліктерін пайдаланатын қауіптерді анықтауды жақсартады.
58. Бағдарламалық жасақтаманың осалдықтарын пайдалануға тырысатын әртүрлі шабуылдарды анықтаудың енгізілген әдістерінің болуы және CVE идентификаторлары туралы толығырақ ақпарат беру.
59. ДК-де бұғатталған IP-мекенжайлардың тізімін қарауға мүмкіндік беретін, қара тізімге түсу себептері туралы ақпарат беретін және нақты қауіпсіз желілік мекенжайлар үшін ерекшеліктер жасауға мүмкіндік беретін дербес брандмауэрдің қосымша функционалының болуы.
60. Жаңа рұқсатсыз желілік қосылымдарға әкеп соққан желілік бағдарламалардағы өзгерістерді анықтауға қабілетті дербес брандмауэрдің қосымша функционалының болуы.
61. Әртүрлі Интернет-трафикті сүзгілеу мүмкіндігі.
62. Сайттардың белгілі бір санаттарына қол жеткізуді шектеуге мүмкіндік беретін веб-бақылау модулінің болуы.
63. Интернет-трафикті сүзгілеудің 27 санатының болуы, оларда 100-ден астам ішкі санаттар бөлінген, сондай-ақ санаттар мен ішкі санаттар бойынша топтарды дербес жасау мүмкіндігі.
64. Түрлі пайдаланушылар мен Windows ОЖ немесе домен топтары үшін Интернет-трафикті сүзгілеу ережелерін жасау мүмкіндігі.
65. Веб-сүзгілеу ережелерін икемді баптауға мүмкіндік береді уақыт аралықтарын (интервалдарын) белгілеу мүмкіндігі.
66. Вирусқа қарсы базаларды тәулігіне кемінде 24 рет регламенттік жаңартуды жүргізу мүмкіндігінің болуы.
67. Интернет желісіне қол жеткізе алмайтын жабық, оқшауланған желілерде антивирустық қорғаныстың өзектілігін сақтауға мүмкіндік беретін сервердегі жергілікті қоймадан клиенттердің жаңартуларын алу мүмкіндігі.
68. Соңғы нүктелерді қорғауға арналған өндірушінің шешімдері негізінде жаңартулар айнасын жасау мүмкіндігі.
69. Егер негізгі жаңарту көзі қолжетімді болмаса, вирус сигнатуралары базасының жаңартуларын резервтік көздерден алу мүмкіндігі.
70. Портативті компьютерлер корпоративтік желіден тыс жерде болған жағдайда, өндірушінің серверлерінен онлайн режимде жаңартуларды алу мүмкіндігі.
71. Вирус сигнатуралары базалары мен жаңарту модульдерінің алдыңғы нұсқаларына қайта оралу мүмкіндігімен жаңартуларды кері шегіндіру (откатить), сондай-ақ жаңартуларды уақытша тоқтатып тұру немесе жаңаларын қолмен орнату функциясының болуы.
72. Тұрақты, тестілік және кейінге қалдырылған жаңартуларды алу режимінде

жаңарту мүмкіндігі.
73. Мониторинг, қауіпсіздік күйін бағалау және әрекет ету құралдарының болуы.
74. Қауіпсіздік күйін және ОЖ жаңартуларының өзектілігін бақылау механизмінің болуы.
75. Іске қосылған процестерді, реестр контентін, орнатылған БЖ-ны, желілік қосылымдарды қоса алғанда, операциялық жүйе жұмысының әртүрлі аспектілерін кейіннен терең талдау үшін операциялық жүйе күйінің суреттерін (снимки состояния) жасай алатын жүйе күйін диагностикалау құралының болуы.
76. Операциялық жүйедегі рұқсатсыз және қауіпті өзгерістерді анықтау мақсатында операциялық жүйенің әртүрлі параметрлері мәндерінің критикалық деңгейін (қауіпті, белгісіз, аз белгілі, қауіпсіз) анықтау мүмкіндігі.
77. Белгілі бір уақыт ішінде жүйеде болған өзгерістерді анықтау мақсатында жүйе күйінің әртүрлі суреттерін салыстыру мүмкіндігі.
78. Қашықтағы ДК-де іске қосылған процестер мен қызметтерді тоқтатуға, реестр тармақтарын жоюға, желілік қосылымдарды бұғаттауға мүмкіндік беретін скрипттерді жасау және қашықтан орындау мүмкіндігі.
79. Жұмыс станцияларында журналдарды жергілікті сақтау мүмкіндігі.

80. Сыртқы бағдарламаны іске қосу, жүйе іске қосылған кезде файлдарды тексеру, жүйе күйінің суретін жасау, компьютерді тексеру, вирус базалары мен бағдарлама модульдерін жаңарту сияқты жоспарланған тапсырмаларды жасауға мүмкіндік беретін тапсырмалар жоспарлағышының болуы.
81. Бір рет, мерзімді түрде, сондай-ақ нақты оқиғалар туындаған жағдайда іске қосылатын тапсырмаларды жоспарлау мүмкіндігі.
82. Жоспарлағышта әртүрлі мерзімділікпен немесе әртүрлі іске қосылу шарттарымен бір типті бірнеше тапсырманы жасау мүмкіндігі.
83. Орнатылған антивирустық өнімі бар CD- және USB-тасымалдағыштарда жүктеу дискісін (загрузочный диск) жасау мүмкіндігі.
84. Соңғы нүктені қорғауға арналған шешімнің параметрлерін құпия сөзбен (парольмен) қорғау мүмкіндігі.
85. Ерекше ортада антивирустық БЖ-ны икемді баптау мақсатында жүйелік әкімшіге ДК-де антивирустық өнімнің саясатпен тағайындалатын және өңдеуге қолжетімсіз параметрлерін уақытша өзгертуге мүмкіндік беретін саясатты қайта анықтау (переопределение политики) режимінің болуы.
86. Жоғары ажыратымдылықты сенсорлық экранмен үйлесімді графикалық интерфейстің болуы.
87. Пайдаланушының жұмыс үстеліндегі оқиғалар туралы хабарландырулар мен хабарламаларды икемді баптау мүмкіндігі.
88. Клиенттік жұмыс станциясына қашықтан орнату мүмкіндігі.
89. Кешенді инсталлятордың көмегімен жекелеген ДК-лерде немесе VDI бейнесінде (образында) алдын ала орнату мүмкіндігі, бұл желіге қосылғаннан немесе VDI ортасында іске қосылғаннан кейін бірден басқару серверімен байланысуға мүмкіндік береді.

90. Әкімшінің немесе пайдаланушының араласуынсыз компоненттерді жүктеуге және орнатуға мүмкіндік беретін компоненттерді автоматты режимде жаңартуға рұқсат ету мүмкіндігі.
91. Басқарылмайтын жұмыс станцияларында компоненттерді жаңартуға мүмкіндік беретін қолмен (ручной) режимде компоненттерді жаңарту мүмкіндігі.
92. Кейбір компоненттердің жұмыс істей бастауы үшін қайта жүктеуді қажет етпей-ақ жаңарту мүмкіндігі.
93. Антивирустық БЖ-дан келетін барлық хабарламаларды жасыру мүмкіндігімен толық экранды режимде жұмыс істейтін бағдарламалардың жұмысын қолдау.
94. Негізгіден басқа, резервтік әкімшілендіру серверлерін көрсету мүмкіндігі.
95. Қашықтан басқару құралының болуы.
96. Өзекті антивирустық өнімнің ДК ресурстарын нақты төмен тұтынуы (барлық процестермен бірге: графикалық интерфейс, кешенді қорғаныс процесі, қашықтан әкімшілендіру қызметі): кемінде 50-100 МБ жедел жад, орталық процессордың 2-35%-ы.
97. Қолдайтын ОЖ (операциялық жүйелер): Microsoft Windows 10/11; Ubuntu Desktop 20.04 LTS (64-биттен кем емес) / 22.04 LTS (64-биттен кем емес) / 24.04 LTS (64-биттен кем емес); Red Hat Enterprise Linux (8/9/10-нан кем емес); Linux Mint (21/22-ден кем емес); Debian (12/13-тен кем емес); MacOS (11/12/13/14/15/26-дан кем емес).

Серверлерді қорғау

1. Серверлік операциялық жүйенің жұмысына әсерді барынша азайтуға мүмкіндік беретін ерекше файлдар, папкалар, қосымшалар үшін автоматты ерекшеліктер жасау мақсатында сервер рөлдерін автоматты түрде анықтау мүмкіндігі.

2. Бағдарламалық жасақтама зиянды бағдарламалардан, трояндық БЖ-дан, пернетақта тыңшыларынан (кейлоггерлерден), жарнамалық БЖ-дан, фишингтен, шпиондық БЖ-дан, руткиттерден, скрипттерден, әлеуетті қажетсіз және қауіпті БЖ-дан қорғанысты қамтамасыз етуі тиіс.
3. Нақты уақыт режимінде қорғанысты қамтамасыз ету функциясының болуы.
4. Бағдарламалық жасақтама сканерлеу кезінде эвристикалық технологияларды пайдалануы тиіс.
5. Пайдаланушының немесе әкімшінің талабы бойынша және кестеге сәйкес антивирустық сканерлеуді жүргізу мүмкіндігі.
6. Сәйкес виртуалды машиналарға қандай да бір агенттерді орнату қажеттілігінсіз Microsoft Hyper-V Server серверінің дискілерін, яғни виртуалды машиналарды (ВМ) сканерлеуге мүмкіндік беретін Hyper-V-ді вирустардың бар-жоғына сканерлеу мүмкіндігін ұсыну.
7. Макростарды зиянды кодтың бар-жоғына тексеруге мүмкіндік беретін

Microsoft Office құжаттарын қорғау модулінің болуы.
8. Java, Flash және басқа да қосымшалардың осалдықтарын пайдалана алатын қауіп-қатерлерден қорғауды қамтамасыз ететін эксплойттардан қорғау.
9. Пайдаланушыларды бопсалаушы бағдарламалардан (ransomware) қорғаудың қосымша деңгейінің болуы, ол барлық бағдарламаларды олардың әрекеті мен беделі негізінде бақылайды және бағалайды.
10. Қосымша бағдарламалық өнімдерді орнату қажеттілігінсіз жұмыс станциялары мен серверлерді қорғауды бұлттық құмсалғышпен (қосымша лицензия болған жағдайда) интеграциялау мүмкіндігі.
11. Негізгі жүктеу жазбасында зиянды бағдарламалық жасақтаманың бар-жоғын тексеру мақсатында UEFI интерфейсін сканерлеу мүмкіндігінің болуы.
12. Операциялық жүйе іске қосылған кезде файлдарды сканерлеу мүмкіндігі.
13. Тіпті мұқият шифрланған және жасырын қауіптердің жұқпалы әсерін болдырмауға мүмкіндік беретін, күдікті процестер пайда болған бойда оларды сканерлейтін және қадағалайтын кеңейтілген жад сканерінің болуы.
14. Компьютерді белсенді емес күйде сканерлеу функциясының болуы.
15. Антивирустық сканер жұмысының егжей-тегжейлі параметрлерін анықтау мүмкіндігі, мысалы, сканерлеу объектілері мен әдістерін анықтау, файлды сканерлеудің максималды өлшемі мен уақытын белгілеу мүмкіндігі, архивтің максималды ішкі салыну тереңдігі және ерекшеліктер жасау.
16. Ауысымдық ақпарат тасымалдағыштарды автоматты түрде антивирустық тексеру функциясының болуы.
17. Құрылғы түрі, әрекеттері, өндірушісі, моделі және құрылғының сериялық нөмірі бойынша ережелерді (саясаттарды) жасау мүмкіндігімен ауысымдық ақпарат тасымалдағыштарды бақылау мүмкіндігі.
18. Құрылғы түрі, қол жеткізу деңгейі, өндірушісі, моделі немесе құрылғының сериялық нөмірі бойынша қол жеткізу ережелерін жасау арқылы жұмыс станциясына перифериялық құрылғылардың қосылуын бақылауды жүзеге асыра алатын құралдың болуы. Ережелерді (саясаттарды) барлық пайдаланушылар үшін де, Windows-тың жекелеген пайдаланушылары немесе пайдаланушылар топтары үшін де жасау мүмкіндігі болуы тиіс.
19. Компьютерді зиянды бағдарламалардан және қажетсіз белсенділіктен қорғайтын басып кіруді анықтау жүйесінің (HIPS) болуы. Сондай-ақ бұл модульде іске қосылған процестерді, пайдаланылатын файлдарды және реестр бөлімдерін бақылау үшін ережелерді жасау шебері мен ережелер редакторы болуы тиіс.

20. Іске қосылған процестерді бұлттық бедел қызметінде қосымша тексеруді жүргізу мүмкіндігі.
21. Жұмыс станциясында пошта клиентін пошта клиентіне интеграциялану мүмкіндігімен қорғауды қамтамасыз ету, POP3, POP3S, SMTP, IMAP және IMAPS хаттамаларын тексеру және пошталық тіркемелерді тексеруді қамтамасыз ету.
22. Зақымдалған поштаны автоматты түрде жою или пошта клиентіндегі

көрсетілген каталогқа ауыстыру мүмкіндігінің болуы.
23. Тексеруден алып тасталған хаттарды, бұғатталған және рұқсат етілген URL-мекенжайларды жасау мүмкіндігімен HTTP, HTTPS трафигін тексеру құралының болуы.
24. Интернеттен файлдарды көрсетілген кеңейтілімі бойынша жүктеуді бұғаттау мүмкіндігі.
25. SSL хаттамасын тексеру және сертификаттардың түпнұсқалығы мен тұтастығын тексеру мүмкіндігі. Сенімді сертификаттар мен тексеруден алып тасталған сертификаттар тізімдерін басқару мүмкіндігі, сондай-ақ сертификат жарамсыз, белгісіз немесе зақымдалған деп анықталған кезде әрекетті таңдау мүмкіндігі.
26. Жекелеген бағдарламалар мен жекелеген IP-объектілер (IP-мекенжайлар, IP-мекенжайлар ауқымы, ішкі желілер) үшін трафикті тексеруден ерекшеліктер жасау мүмкіндігі.
27. Компьютерге жасалуы мүмкін желілік шабуылдардың әртүрлі түрлерін анықтау үшін басып кіруді анықтау жүйесі (IDS) модулінің қосымша параметрлерін баптау мүмкіндігі.
28. «Ботнет» типті қауіп-қатерлерден қорғанысты қамтамасыз ететін технологияны пайдалану мүмкіндігі.
29. Желілік хаттамалардың осалдықтарын қорғау, бұл SMB, RPC, RDP және т.б. сияқты желілік хаттамалардың кемшіліктерін пайдаланатын қауіптерді анықтауды жақсартады.
30. Вирусқа қарсы базаларды тәулігіне кемінде 24 рет регламенттік жаңартуды жүргізу мүмкіндігінің болуы.
31. Клиенттік құрылғылар үшін жаңартуды сервердегі жергілікті айнадан алу.
32. Антивирустық БЖ құралдарымен жаңарту айнасын жасау мүмкіндігі.
33. Егер негізгі жаңарту көзі қолжетімді болмаса, вирус базаларын резервтік көздерден жаңарту мүмкіндігі.
34. Вирус сигнатуралары базалары мен жаңарту модульдерінің алдыңғы нұсқаларына қайта оралу мүмкіндігімен жаңартуларды кері шегіндіру функциясының болуы, сондай-ақ жаңартуларды уақытша тоқтатып тұру немесе жаңаларын қолмен орнату мүмкіндігі.
35. Тұрақты, тестілік және кейінге қалдырылған жаңартуларды алу режимінде жаңарту мүмкіндігі.
36. Қашықтан басқару құралының болуы.
37. Негізгіден бөлек, резервтік әкімшілендіру серверлерін көрсету мүмкіндігі.
38. Операциялық жүйе жаңартуларының өзектілігін бақылау механизмінің болуы.
39. Іске қосылған процестерді, реестр контентін, орнатылған БЖ-ны, желілік қосылымдарды қоса алғанда, операциялық жүйе жұмысының әртүрлі аспектілерін кейіннен терең талдау үшін операциялық жүйе күйінің суреттерін жасай алатын жүйені диагностикалау құралының болуы. Жүйе күйінің әртүрлі суреттерін салыстыру мүмкіндігінің арқасында бұл құрал жүйеде болған өзгерістерді анықтай алады. Сондай-ақ ол іске қосылған процестерді тоқтатуға, реестр тармақтарын жоюға, желілік қосылымдарды бұғаттауға

мүмкіндік беретін скрипттерді жасап, орындай алады.
40. Сыртқы бағдарламаны іске қосуды, жүйе іске қосылған кезде файлдарды тексеруді, жүйе күйінің суретін жасауды, компьютерді тексеруді, вирус базалары мен бағдарлама модульдерін жаңартуды қоса алғанда, жоспарланған тапсырмаларды жасауға мүмкіндік беретін тапсырмалар жоспарлағышының болуы.

Бір рет, мерзімді түрде және нақты оқиғалар туындаған кезде іске қосылатын тапсырмаларды жоспарлау мүмкіндігі.
41. Жоспарлағышта әртүрлі мерзімділікпен немесе әртүрлі іске қосылу шарттарымен бір типті бірнеше тапсырманы жасау мүмкіндігі.
42. Доменде де, жұмыс тобында (рабочая группа) да кластерлерде жұмыс істеу мүмкіндігі.
43. Сканерлеу ағындарының (потоков сканирования) санын көрсете отырып, жылдамдықты баптау мүмкіндігі.
44. Терминалдық пайдаланушылар үшін графикалық интерфейсті ажырату арқылы іске қосу режимін баптау мүмкіндігі, бұл терминалдар сервері режимінде жұмыс істейтін серверге түсетін жүктемені азайтуға мүмкіндік береді.
45. Орнатылған антивирустық өнімі бар CD- және USB-тасымалдағыштарда жүктеу дискісін жасау мүмкіндігі.
46. Антивирустық БЖ-дан келетін барлық хабарламаларды жасыру мүмкіндігімен толық экранды режимде жұмыс істейтін бағдарламалардың жұмысын қолдау.
47. Антивирустық БЖ параметрлерін өзгертуден және жоюдан құпия сөзбен (парольмен) қорғау мүмкіндігі.
48. Серверге қашықтан орнату мүмкіндігі.
49. Кешенді инсталлятордың көмегімен жекелеген серверлерде алдын ала орнату мүмкіндігі, бұл желіге қосылғаннан кейін бірден басқару серверімен байланысуға мүмкіндік береді.
50. Microsoft Azure бұлттық сервисімен интеграциялану мүмкіндігі.
51. Қолдайтын ОЖ (операциялық жүйелер): Microsoft Windows Server (2025/2022/2019/2016/2012 R2/2012-ден кем емес); Red Hat Enterprise Linux (RHEL) (8/9/10-нан кем емес); Rocky Linux v.8 / v.9 / v.10; Ubuntu Server 22.04 LTS / 24.04 LTS; Debian 11 / 12 / 13; SUSE Linux Enterprise Server (SLES) 15 / 16; Alma Linux (8/9/10-нан кем емес); Rocky Linux

---

(8/9/10-нан кем емес); Oracle Linux (8/9/10-нан кем емес); Amazon Linux (2023-тен кем емес).

Заңнама талаптары

1. Ұсынылатын бағдарламалық шешім сенімділігі мен қауіпсіздігі бойынша осы салаға жататын халықаралық стандарттарға, стандарттарға және техникалық регламенттерге сәйкес болуы тиіс.