ТЕХНИКАЛЫҚ СИПАТТАМА

1268301 сатып алу бойынша
Төмендету баға ұсыныстарын сұрату тәсілімен

Лот № (76 Т, 4575372) Лицензия

Тапсырыс беруші: ТОО "КазРосГаз"
Ұйымдастырушы: ТОО "КазРосГаз"

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	76 Т
Атауы және қысқаша сипаттамасы	Лицензия, бағдарламалық өнімге (лицензия беру қызметінен басқа)
Қосымша сипаттама	Түрі: антивирустық бағдарламаның жылдық лицензиясы
Саны	1.000
Өлшем бірлігі	Дана
Жеткізу орны	ҚАЗАҚСТАН, Алматы қ., ул.Байзакова, 280
Жеткізу шарттары	DDP
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап (қоса алғанда) 12.2026 дейін.
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

70 пайдаланушыға жұмыс станцияларын, серверлерді және мобильді құрылғыларды қорғау үшін антивирустық бағдарламалық жасақтаманы пайдалану құқығына лицензия беру.

Берілген лицензияның қолданылу мерзімі лицензия берілген күннен бастап кемінде бір күнтізбелік жылды құрауы тиіс.

Kaspersky бағдарламалық жасақтамасын пайдалануға жарамды лицензия бар. Барлығы Қауіп сіздік үшін 70 пайдаланушыға арналған бизнес .

Антивирустық құралдар мыналарды қамтуы керек:

- Windows жұмыс станцияларына арналған антивирустық қорғау бағдарламалық жасақтамасы;
- Windows файл серверлеріне арналған антивирустық қорғау бағдарламалық жасақтамасы;
- MacOS жұмыс станцияларына арналған антивирустық қорғау бағдарламалық жасақтамасы ;
- Linux жұмыс станциялары мен серверлеріне арналған антивирустық қорғау бағдарламалық жасақтамасы;
- мобильді құрылғыларға (смартфондар мен планшеттерге) арналған антивирустық қорғау бағдарламалық жасақтамасы;

- веб-трафикті қорғауға арналған антивирустық бағдарламалық жасақтама;
- Бөлек серверді пайдаланатын антивирустық қорғаныс және спамды сүзу бағдарламалық жасақтамасы
- Linux пошта серверлеріне арналған антивирустық қорғау және спамды сүзу бағдарламалық жасақтамасы;
- Microsoft Exchange серверлеріне арналған антивирустық қорғау және спамды сүзу бағдарламалық жасақтамасы;
- орталықтандырылған басқару, мониторинг және жаңарту үшін бағдарламалық жасақтама;
- зиянды бағдарламалар мен шабуыл қолтаңбаларының жаңартылған дерекқорлары;
- пайдалану құжаттамасы орыс тілінде.

Басқару құралдарын қоса алғанда, барлық антивирустық бағдарламалық жасақтаманың бағдарламалық интерфейсі орыс және ағылшын тілдерінде қолжетімді болуы керек. Басқару құралдарын қоса алғанда, барлық антивирустық бағдарламалық жасақтаманың орыс және ағылшын тілдерінде контекстке сезімтал анықтама жүйесі болуы керек.

Windows жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама талаптары

Вирусқа қарсы бағдарламалық жасақтама жұмыс станциясының операциялық жүйесінің келесі нұсқаларын іске қосатын компьютерлерде жұмыс істеуі керек:

1. Windows 7 Home/Professional/Ultimate/Enterprise Service Pack 1 және одан жоғары нұсқасы ;
2. Windows 8 Professional/Enterprise (32/64 бит);
3. Windows 8.1 Professional/Enterprise (32/64 бит);
4. Windows 10 Home/Pro/Pro үшін жұмысшылар станциялар / Білім беру / Кәсіпорын /Кәсіпорын көп сессиялы;
5. Windows 11 Home/Pro/Pro үшін жұмысшылар станциялар / Білім беру / Кәсіпорын;
6. Windows 11 Pro / Pro үшін жұмысшылар станциялар / Білім беру / Кәсіпорын.

Вирусқа қарсы бағдарламалық жасақтама келесі функцияларды орындауы керек:

- нақты уақыт режимінде және нысанның контекстік мәзірінен сұраныс бойынша антивирустық сканерлеу;
- жоспарланған антивирустық сканерлеу;
- қосылған құрылғыларды антивирустық сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- белсенді инфекцияның әсерін бейтараптандыру;
- қолданбаның зиянды әрекетін анықтау және рұқсатсыз әрекеттерді анықтау үшін оның әрекетін және жүйеде орындайтын әрекеттерін талдау;
- желі арқылы қолжетімді қорғалған ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қол жеткізуді талдау;

- ортақ қалталарды сыртқы шифрлаудан қорғау функциясы үшін қорғаныс ауқымын жасау;
- бағдарламалық жасақтамадағы осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, соның ішінде жүйелік процестердің жадын қорғау;
- зиянды бағдарламамен шифрланған файлдарды қалпына келтіруді қоса алғанда, өңдеу кезіндегі зиянды бағдарламалардың әрекеттерін кері қайтару;
- процестер мен қолданбалар үшін артықшылықтарды шектеулер (тізілімге жазу, файлдарға, қалталарға және басқа процестерге кіру, тапсырма жоспарлағышына кіру, құрылғыларға кіру, нысандарға құқықтарды өзгерту және т.б.), анықталған сенім деңгейімен динамикалық түрде жаңартылатын қолданбалардың теңшелетін тізімдері;
- жаңа қауіптерден бұлтқа негізделген қорғаныс, бұл қолданбаға іске қосылып жатқан бағдарлама немесе файл туралы шешім алу үшін өндірушінің ресурстарына нақты уақыт режимінде қол жеткізуге мүмкіндік береді;
- келесі форматтағы мұрағаттардағы файлдарды антивирустық сканерлеу және өңдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- IMAP, SMTP, POP3, MAPI, NNTP хаттамалары арқылы берілетін кіріс және шығыс трафикті сканерлеу арқылы электрондық поштаны зиянды бағдарламалардан қорғау;
- көрсетілген файл түрлерінің атын өзгерту немесе жою мүмкіндігі бар пошта тіркемесінің сүзгісі;
- пайдаланушының компьютеріне HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP және FTP хаттамалары арқылы келетін желілік трафикті тексеру, соның ішінде сенімді ресурстарды конфигурациялау және блоктау немесе статистика режимінде жұмыс істеу мүмкіндігімен эвристикалық талдауды пайдалану;
- жүктелген веб-беттердегі баннерлерді және қалқымалы терезелерді бұғаттау;
- фишингтік және қауіпсіз емес веб-сайттарды тану және бұғаттау;
- желілік сегменттерді жіктеу мүмкіндігімен бағдарламаларға арналған желілік пакет ережелерін және желілік ережелерді жасауға мүмкіндік беретін кіріктірілген брандмауэр;
- кез келген типтегі есептеу желілеріндегі қолданбалар мен порттарға арналған брандмауэр ережелерін пайдалана отырып, желілік шабуылдардан қорғау;
- ARP хаттамасындағы осалдықтарды құрылғының MAC мекенжайын бұрмалау үшін пайдаланатын желілік қауіптерден қорғау;
- бірнеше желілік қосылымдардың бір уақытта орнатылуын блоктау мүмкіндігімен желілік көпір түріндегі желілік қосылымдарды басқару;
- барлық немесе нақты пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді жасау арқылы компонент қолданбаларды бағдарламаның жолы, метадеректері, сертификаты немесе оның саусақ ізі, бақылау қосындысы бойынша да, бағдарламалық жасақтама өндірушісі ұсынған алдын ала анықталған қолданбалар санаттары бойынша да бақылауы керек, компонент қара тізім немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе бұғаттау режимінде жұмыс істеуі керек;
- пайдаланушының сыртқы енгізу/шығару құрылғыларымен жұмысын құрылғы түрі және/немесе пайдаланылатын шина бойынша басқару, сенімді құрылғылардың тізімін

олардың идентификаторы бойынша жасау және Active Directory-ден белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалануға құқықтар беру мүмкіндігі;
- құрылғыны басқару бөлігі ретінде MTP құрылғыларын басқару және осы типтегі құрылғыларға барлық немесе пайдаланушы топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін кіру ережелерін орнату;
- алынбалы дискілердегі файлдарды жазу және/немесе жою туралы оқиғалар журналындағы жазбалар;
- файлдық жүйесі бар құрылғыларға кіру ережелеріне басымдық беру;
- пайдаланушының Интернетпен жұмысын бақылау, соның ішінде санаттарды қосу және өңдеу, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық түрде жаңартылатын санаттарға, сондай-ақ ақпарат түріне (аудио, бейне және т.б.) қол жеткізуге нақты тыйым салуды немесе рұқсат беруді қосу, басқару үшін уақыт аралықтарын енгізуге және оны тек Active Directory-ден белгілі бір пайдаланушыларға тағайындауға мүмкіндік беру;
- BadUSB типті шабуылдардан қорғау ;
- қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ құпия сөзді пайдаланып қолданба параметрлеріне кіруді қорғау;
- сенімді қашықтан басқару бағдарламалары арқылы параметрлерді басқару;
- антивирустық бағдарламалық жасақтаманың тек таңдалған компоненттерін орнату;
- жоғарыда аталған барлық компоненттерді бірыңғай басқару жүйесін пайдаланып орталықтандырылған басқару;
- кесте бойынша және/немесе қолданба іске қосылғаннан кейін бірден тапсырмаларды орындау;
- Файл кеңістігін сканерлеу кезінде пайдаланушының ыңғайлы тәжірибесін қамтамасыз ету үшін компьютерлік ресурстарды пайдалануды икемді басқару;
- соңғы сканерлеуден бері мәртебесі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- антивирустық бағдарламаның тұтастығын тексеру;
- файлды тексеру сомасына, атауға/каталог маскасына немесе файлдың сенімді сандық қолтаңбасы бар-жоғына негізделген антивирустық сканерлеуден алып тастауларды қосу;
- XML форматындағы ережелер мен ерекшеліктер тізімдерін импорттау және экспорттау;
- антивируста жойылған вирус жұққан файлдарды қалпына келтіру мүмкіндігі бар қорғалған сақтау орны бар;
- антивирустық жұмыс туралы есептерді қауіпсіз сақтау орнының болуы;
- антивирустық графикалық интерфейсті қосу және өшіру, сондай-ақ минималды мүмкіндіктер жиынтығы бар графикалық интерфейстің жеңілдетілген нұсқасының болуы;
- интеграция Windows Defender қауіпсіздік орталығымен ;
- қолжетімділік Зиянды бағдарламаларға қарсы сканерлеу интерфейсін (AMSI) қолдау ;
- қолжетімділік Linux үшін Windows ішкі жүйесін (WSL) қолдау ;
- резервтік көшірмеден нысандарды қалпына келтіруді құпия сөзбен қорғау;
- интернет байланысы шектеулі болған жағдайда желілік трафикті шектеу;
- TCP және UDP хаттамалары үшін желілік мониторинг құралының болуы ;

- сканерлеу үзілген жерден қайта жүктегеннен кейін сканерлеу тапсырмасын жалғастырыңыз;
- тапсырманың ұзақтығына шектеу қою;
- егер сканерлеу қазірдің өзінде жұмыс істеп тұрса, сканерлеу тапсырмаларын кезекке қою;
- жүйені қайта жүктемей жаңарту;
- Android қолданбасында пайдаланушының мобильді құрылғыларға кіруін орнатыңыз Жөндеу көпірі (ADB);
- мобильді құрылғыңызға кіру мүмкіндігі бұғатталған болса да, мобильді құрылғыңызды USB арқылы компьютерге қосу арқылы зарядтаңыз;
- пайдаланушылар үшін басып шығару құқықтарын орнату;
- Wi -Fi желілеріне қосылымдарды басқару үшін WPA3 хаттамасын қолдаудың болуы ;
- Azure WVD-мен үйлесімділік;
- iTunes қолданбасында пайдаланушының мобильді құрылғыларға кіруін конфигурациялау ;
- Компьютеріңізде орнатылған қолданбалардағы осалдықтарды анықтау және түзету үшін анықталған осалдықтар туралы есеп жасау мүмкіндігімен арнайы тапсырманы іске қосыңыз.
- Арнайы жүктеу агентін жасау және бірыңғай кіру технологиясын қолдау, UEFI жүйелерін қолдау арқылы толық дискілік шифрлау;
- жүктеу агентінің немесе ОС файлдарының істен шығуы жағдайында шифрланған мазмұнды қалпына келтіру, UEFI жүйелерін қолдау;
- толық дискілік шифрлаумен екі факторлы аутентификацияны қолдау ;
- шифрланатын мазмұнды икемді түрде көрсету мүмкіндігімен файлдарды шифрлау (орналасқан жері бойынша, кеңейтімі бойынша, файлды жасаған қолданба бойынша);
- таңдалған қолданбалардан шифрланған файлдарға қол жеткізуді шектеу механизмдерінің болуы, сондай-ақ файлдарды ұйымнан тыс жерде құпия сөзді пайдаланып шифрдан шығаруға мүмкіндік беретін технологияның болуы;
- ұйым желісінен тыс файлдарды шифрлауға және шифрын ашуға мүмкіндік беретін жұмыс режимін орнату мүмкіндігімен алынбалы тасымалдағыштардағы деректерді шифрлау;
- бағдарламалар үшін мінез-құлық үлгісін қалыптастыру және олардың мінез-құлық үлгісінен ауытқыған жағдайда әрекеттерін бұғаттау мүмкіндігі (бейімделгіш аномалияны бақылау)
- дискіні шифрлау кезінде аутентификация агенті үшін қызметтік тіркелгі жасау мүмкіндігі;
- Толық дискілік шифрлаумен SSO үшін үшінші тарап тіркелгі деректерін жеткізуші ADSelfService Plus қолдауы ;
- енгізу құрылғыларынан басқа барлық Bluetooth құрылғыларына ерекше жағдайларды орнату және кіруді шектеу мүмкіндігі;
- операциялық жүйені қайта жүктемей қолданбаны жаңарту мүмкіндігі;
- зиянды бағдарламаны іздеу тапсырмасы үшін процессор ресурстарын тұтынуды шектеу мүмкіндігі;
- қолданбалы қызметтерді сыртқы басқаруға тыйым салу мүмкіндігі;

- алдын ала орнатылған сканерлеу ерекшеліктерін және сенімді қолданбаларды таңдау мүмкіндігі;
- жеке пайдаланушыға параметрлерді конфигурация файлына экспорттауға рұқсат беру мүмкіндігі;
- қолданбаға кіруге арналған уақытша құпия сөздерді бақылау және жою мүмкіндігі, бұл сізге құпия сөз тарихын сақтауға (30 күнге дейін) және күйін басқаруға мүмкіндік береді (Белсенді , Мерзімі өткен , Қайтарып алынған);
- саясат қолданылғаннан кейін бірден Web Control ережелерімен тыйым салынған веб-ресурстарға қосылымдарды ажырату мүмкіндігі;
- орнату пакетіндегі әртүрлі операциялық жүйелер түрлері үшін әртүрлі компоненттер жиынтығын конфигурациялау мүмкіндігі;
- алдын ала орнатылған сканерлеу ерекшеліктерін және сенімді қолданбаларды таңдау мүмкіндігі;
- ескірген TLS 1.0 протоколын пайдаланып желілік қосылымдарды бұғаттау мүмкіндігі;
- Интернетке кіру үшін прокси-сервер арқылы қолданбаны аутентификациялау үшін Kerberos хаттамасын қолдау ;
- қолданбаны сканерлеуден шығару үшін файл хэшін көрсету мүмкіндігі .

Windows серверлеріне арналған антивирустық бағдарламалық жасақтама талаптары

Вирусқа қарсы қорғау бағдарламалық жасақтамасы файл серверінің операциялық жүйесінің келесі нұсқаларын іске қосатын компьютерлерде жұмыс істеуі керек:

1. Windows Small Business Server 2011 Essentials / Standard (64-бит), Microsoft Small Business Server 2011 Standard (64-бит) қолдау көрсетіледі тек Microsoft Windows Server 2008 R2 үшін 1-ші қызмет көрсету бумасы орнатылған кезде ғана;
2. Windows MultiPoint Server 2011 (64-бит);
3. Windows Server 2008 R2 Foundation/Standard/Enterprise/Datacenter Service Pack 1 және одан жоғары нұсқасы ;
4. Windows Web Server 2008 R2 Service Pack 1 және одан жоғары нұсқасы ;
5. Windows Server 2012 Foundation / Essentials / Standard / Datacenter (соның ішінде) Сервердің негізгі режимі);
6. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (соның ішінде) Сервердің негізгі режимі);
7. Windows Server 2016 Essentials / Standard / Datacenter (соның ішінде) Сервердің негізгі режимі);
8. Windows Server 2019 Essentials / Standard / Datacenter (соның ішінде) Сервердің негізгі режимі);
9. Windows Server 2022 Standard / Деректер орталығы / Деректер орталығы: Azure Edition (соның ішінде) Сервердің негізгі режимі).
10. Windows Server 2025 Standard / Деректер орталығы.

Вирусқа қарсы бағдарламалық жасақтама келесі функцияларды орындауы керек:

- нақты уақыт режимінде және нысанның контекстік мәзірінен сұраныс бойынша антивирустық сканерлеу;
- жоспарланған антивирустық сканерлеу;
- қосылған құрылғыларды антивирустық сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- белсенді инфекцияның әсерін бейтараптандыру;
- қолданбаның зиянды әрекетін анықтау және рұқсатсыз әрекеттерді анықтау үшін оның әрекетін және жүйеде орындайтын әрекеттерін талдау;
- желі арқылы қолжетімді қорғалған ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қол жеткізуді талдау;
- бағдарламалық жасақтамадағы осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, соның ішінде жүйелік процестердің жадын қорғау;
- зиянды бағдарламамен шифрланған файлдарды қалпына келтіруді қоса алғанда, өңдеу кезіндегі зиянды бағдарламалардың әрекеттерін кері қайтару;
- жаңа қауіптерден бұлтқа негізделген қорғаныс, бұл қолданбаға іске қосылып жатқан бағдарлама немесе файл туралы шешім алу үшін өндірушінің ресурстарына нақты уақыт режимінде қол жеткізуге мүмкіндік береді;
- келесі форматтағы мұрағаттардағы файлдарды антивирустық сканерлеу және өңдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- желілік сегменттерді жіктеу мүмкіндігімен бағдарламаларға арналған желілік пакет ережелерін және желілік ережелерді жасауға мүмкіндік беретін кіріктірілген брандмауэр;
- ARP хаттамасындағы осалдықтарды құрылғының MAC мекенжайын бұрмалау үшін пайдаланатын желілік қауіптерден қорғау;
- қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ қолданба параметрлеріне кіруді құпия сөзбен қорғау, зиянды бағдарламалардың, зиянкестердің немесе білікті емес пайдаланушылардың қорғауды өшіруіне жол бермеу;
- антивирустық бағдарламалық жасақтаманың тек таңдалған компоненттерін орнату;
- жоғарыда аталған барлық компоненттерді бірыңғай басқару жүйесін пайдаланып орталықтандырылған басқару;
- тапсырмаларды кесте бойынша және/немесе операциялық жүйені жүктегеннен кейін бірден іске қосу;
- Файл кеңістігін сканерлеу кезінде пайдаланушының ыңғайлы тәжірибесін қамтамасыз ету үшін компьютерлік ресурстарды пайдалануды икемді басқару;
- соңғы сканерлеуден бері мәртебесі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- антивирустық бағдарламаның тұтастығын тексеру;
- файлды тексеру сомасына, атауға/каталог маскасына немесе файлдың сенімді сандық қолтаңбасы бар-жоғына негізделген антивирустық сканерлеуден алып тастауларды қосу;
- антивируста жойылған вирус жұққан файлдарды қалпына келтіру мүмкіндігі бар қорғалған сақтау орны бар;
- антивирустық жұмыс туралы есептерді қауіпсіз сақтау орнының болуы;

- антивирустық графикалық интерфейсті қосу және өшіру, сондай-ақ минималды мүмкіндіктер жиынтығы бар графикалық интерфейстің жеңілдетілген нұсқасының болуы;
- интеграция Windows Defender қауіпсіздік орталығымен ;
- қолжетімділік Зиянды бағдарламаларға қарсы сканерлеу интерфейсін (AMSI) қолдау ;
- қолжетімділік Linux үшін Windows ішкі жүйесін (WSL) қолдау ;
- Сақтық көшірме сақтау орнынан нысандарды қалпына келтіру үшін құпия сөзді пайдаланыңыз.
- XML форматындағы ережелер мен ерекшеліктер тізімдерін импорттау және экспорттау;
- интернет байланысы шектеулі болған жағдайда желілік трафикті шектеу;
- барлық немесе нақты пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді жасау, компонент қолданбаларды бағдарламаның жолы, метадеректері, сертификаты немесе оның саусақ ізі, бақылау қосындысы бойынша да, бағдарламалық жасақтама өндірушісі ұсынған қолданбалардың алдын ала анықталған санаттары бойынша да басқаруы керек, компонент қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе блоктау режимінде жұмыс істеуі керек;
- бағдарламалар үшін мінез-құлық үлгісін қалыптастыру және егер олар мінез-құлық үлгісінен ауытқып кетсе, олардың әрекеттерін бұғаттау (бейімделгіш аномалияны бақылау);
- компьютерде орнатылған қолданбалардағы осалдықтарды анықтау және жабу үшін анықталған осалдықтар туралы есеп беру мүмкіндігімен арнайы тапсырманы іске қосу;
- Серверлерге арналған Windows операциялық жүйесін іске қосатын компьютерлерге арналған веб-қауіптен қорғау, поштаға қауіптен қорғау, веб-бақылау және құрылғыны басқару компоненттерін қолдау.
- сканерлеу үзілген жерден қайта жүктегеннен кейін сканерлеу тапсырмасын жалғастырыңыз;
- тапсырманы орындау үшін уақыт шегін белгілеу мүмкіндігі;
- егер сканерлеу қазірдің өзінде жұмыс істеп тұрса, сканерлеу тапсырмаларын кезекке қою мүмкіндігі;
- жүйені қайта жүктемей жаңарту;
- портативті құрылғыларға (PT) кіру құқықтарын (оқу/жазу) орнату, құрылғыларға кіру мүмкіндігі бар пайдаланушыларды немесе пайдаланушылар тобын таңдау және құрылғыларға кіру кестесін белгілеу;
- мобильді құрылғыңызға кіру мүмкіндігі бұғатталған болса да, оны USB арқылы компьютерге қосу арқылы мобильді құрылғыңызды зарядтаңыз;
- пайдаланушылар үшін басып шығару құқықтарын орнату;
- Wi -Fi желілеріне қосылымдарды басқару үшін WPA3 хаттамасын қолдаудың болуы ;
- Azure WVD-мен үйлесімділік;
- операциялық жүйені қайта жүктемей қолданбаны жаңарту мүмкіндігі ;
- зиянды бағдарламаны қарап шығу тапсырмасы үшін CPU ресурстарын тұтынуды шектеу мүмкіндігі.

- қолданбалы қызметтерді сыртқы басқаруға тыйым салу мүмкіндігі.
- SQL серверлерінде, Microsoft Exchange серверлерінде және System Center Configuration Manager бағдарламасында қолданбалардың жұмыс істеуі үшін сенімді аймақты жылдам конфигурациялауға арналған алдын ала анықталған сканерлеуді алып тастауларды және сенімді қолданбаларды пайдалану мүмкіндігі;
- Интернетке кіру үшін прокси-сервер арқылы қолданбаны аутентификациялау үшін Kerberos хаттамасын қолдау ;
- қолданбаны сканерлеуден шығару үшін файл хэшін көрсету мүмкіндігі .

Мас жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама талаптары

Мас жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі керек:

1. macOS 12 - 15 ;

Вирусқа қарсы бағдарламалық жасақтама келесі функцияларды орындауы керек:

- резиденттік антивирустық мониторинг;
- Жаңа қауіптерден бұлтқа негізделген қорғаныс, қолданбаға іске қосылып жатқан бағдарлама немесе файл туралы шешім алу үшін өндірушінің арнайы ресурстарына нақты уақыт режимінде қол жеткізуге мүмкіндік береді;
- антивирустық дерекқорларды автоматты түрде жоспарлы түрде жаңарту;
- қалпына келтіруді қамтамасыз ету үшін вирус жұққан файлдарды жоймас бұрын олардың сақтық көшірмесін жасаңыз;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- кез келген компьютерлік желіде, соның ішінде сымсыз желіде жұмыс істеген кезде ең танымал қолданбалар үшін басып кіруді анықтау және алдын алу жүйесін (IDS/IPS) және желілік белсенділік ережелерін пайдаланып желілік шабуылдардан қорғау;
- Антивирустық бағдарламалық жасақтама өндірушісінің беделді бұлттық қызметтерінің шешімдеріне негізделген зиянды және фишингтік веб-сайттарды бұғаттау;
- Chrome және Firefox браузерлері арқылы берілетін желілік трафикті тексеру (HTTP және HTTPS трафигі);
- пайдаланушының Интернеттегі жұмысын бақылау, соның ішінде санаттарды қосу және өңдеу, өндіруші жасаған және динамикалық түрде жаңартылған белгілі бір ресурстарға немесе ресурстар санаттарына кіруге нақты тыйым салуды немесе рұқсат беруді қосу
- соңғы сканерлеуден бері мәртебесі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- файл операциясын ұстап алу деңгейінде көрсетілген аймақтарды тексеру кезінде ерекше жағдайларды орнату ;
- дискіге толық кіру құқықтарының пайда болуын автоматты түрде бақылайды және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнатады;

- зиянды бағдарламаларды сканерлеу тапсырмаларын орындау кезінде қолданбаның процессорлық процессорды пайдалануын шектеу;
- бұлттық режимді қосу және операциялық жүйе ресурстарына жүктемені азайту үшін зиянды бағдарламалар дерекқорларының жеңіл нұсқасын пайдалану;
- Сұраныс бойынша сканерлеу тапсырмаларын орындаған кезде тек оқуға арналған жүйе көлемін сканерлеуді өткізіп жіберу;
- BSS) қолдана отырып, операциялық жүйедегі қолданбалы белсенділікті талдау ;
- .pkg файлынан орнату ;
- сыртқы дискілер қосылған кезде оларды автоматты түрде сканерлеу;
- клиенттік сертификаттарды қолдау ;
- кіріс және шығыс электрондық пошта хабарламаларының қосымшаларын зиянды заттар мен басқа да қауіптерге тексеру;
- компьютерге орнатылған немесе қосылған құрылғыларға пайдаланушының кіруін басқару;
- интернетте немесе жергілікті желіде жұмыс істеген кезде компьютеріңізге рұқсатсыз қосылымдарды бұғаттау және қолданбалардың желілік белсенділігін бақылау;
- ОС-тағы файлдық, жүйелік немесе желілік белсенділікке қатысты зиянды бағдарламалық жасақтама әрекеттерін кері қайтару;
- пайдаланудан қорғау ;
- жоғарыда аталған барлық компоненттерді бірыңғай басқару жүйесін пайдаланып орталықтандырылған басқару.

Linux жұмыс станциялары мен серверлеріне арналған антивирустық бағдарламалық жасақтама талаптары

Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі 32 биттік операциялық жүйелерді іске қосатын компьютерлерде жұмыс істеуі керек:

1. Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі 64 биттік операциялық жүйелерді іске қосатын компьютерлерде жұмыс істеуі керек:

1. AlmaLinux ОЖ 8.6, 8.7, 8.8, 8.9.
2. AlmaLinux OS 9.4, 9.5, 9.6.
3. AlterOS® 2025.
4. Amazon™ Linux 2023.
5. Astra Linux жалпы басылымы 2.12.
6. Astra Linux арнайы басылымы RUSB.10015-01 (басқа 1.5 жаңартуы).
7. Astra Linux арнайы басылымы RUSB.10015-01 (басқа 1.6 жаңартуы).
8. Astra Linux арнайы басылымы RUSB.10015-01 (басқа 1.7 жаңартуы).
9. Astra Linux арнайы басылымы RUSB.10015-01 (басқа 1.8 жаңартуы).
10. Astra Linux арнайы басылымы RUSB.10015-03 (келесі 7.6 жаңартуы).
11. Астра Linux Арнайы RUSB.10015-16 басылымы (1-нұсқа) (соңғы жаңарту 1.6).
12. Astra Linux арнайы басылымы RUSB.10015-17 (басқа жаңарту 1.7.3).
13. Astra Linux арнайы басылымы RUSB.10015-37 (басқа 7.7 жаңартуы).

14. CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
15. CentOS ағыны 8.
16. CentOS ағыны 9.
17. CentOS ағыны 10.
18. Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
19. Debian GNU/Linux 13.0, 13.1, 13.2.
20. EMIAS 1.0.
21. EulerOS 2.0 SP10.
22. Федора 41.
23. Килин 10.
24. Linux Mint 21.3.
25. Linux Mint 22.2.
26. Mostech 12 нұсқасының 2021.1 нұсқасы.
27. openSUSE Leap 15.6.
28. Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
29. Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9.
30. Oracle Linux 9.4, 9.5, 9.6.
31. Red Hat® Enterprise Linux® 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
32. Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9.
33. Red Hat Enterprise Linux 9.4, 9.5, 9.6.
34. Red Hat Enterprise Linux 10.0, 10.1.
35. Rocky Linux 8.6, 8.7, 8.8, 8.9.
36. Rocky Linux 9.4, 9.5, 9.6.
37. SberLinux 8.10, 9.1, 9.5, 9.6.
38. SberOS 3.4.0, 3.5.0.
39. SUSE Linux Enterprise Server 12.5, 12.6, 12.7.
40. SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7.
41. Ubuntu® 22.04 LTS.
42. Ubuntu 24.04 LTS.
43. Альто Білім беру 10.
44. Альто Білім беру 11.
45. Альто Жұмыс істеп тұр 11-ші станция .
46. Альто 11- сервер .
47. Alt SP сервері 10-шы шығарылым .
48. Alt SP жұмыс станциясының 10-шығарылымы.
49. Atlant , Alcyone құрастыру , 2022.02 нұсқасы .
50. GosLinux 7.2.
51. MOS 12 серверінің 2021.1 нұсқасы.
52. MosOS 15.5 Arbat.
53. MSVSFERA 9.4 ARM.
54. MSVSPHERE 9.4 СЕРВЕРІ.
55. OS MESH 12 Барлық пайдаланушылар үшін (телеметриясыз және DIT қолдауынсыз) 2021.1 нұсқасы .
56. Мәскеу мектептеріне арналған интерактивті панельдерге арналған OS MESH 12 (телеметрия және DIT қолдауымен) 2021.1 шығарылымы .

57. Мәскеу мектептеріне арналған компьютерлер мен ноутбуктерге арналған OS MESH 12 (телеметрия және DIT қолдауымен) 2021.1 шығарылымы .
58. НЕГІЗІ .
59. ОС 3.0.5.
60. ҚЫЗЫЛ OS® 7.3.
61. ҚЫЗЫЛ ОС 8.0.
62. ROSA " Кобальт " 7.9 жұмыс істейді станция .
63. ROSA " Cobalt " 7.9 Сервер .
64. ROSA " Chrome " 12 жұмыс істейді станция .
65. ROSA " Chrome " 12 сервері .
66. SynthesisM-Client 8.6.
67. SynthesisM-Server 8.6.

A RM архитектурасы үшін қолдау көрсетілетін 64-биттік операциялық жүйелер :

1. Astra Linux арнайы басылымы RUSB.10152-02 (соңғы жаңарту 4.7).
2. CentOS ағыны 9.
3. EulerOS 2.0 SP10.
4. SUSE Linux Enterprise Server 15.
5. Ubuntu 22.04 LTS.
6. Alt SP жұмыс станциясының 10-шығарылымы.
7. Alt SP серверінің 10-шығарылымы.
8. ҚЫЗЫЛ ОС 8.0.

Вирусқа қарсы бағдарламалық жасақтама келесі функцияларды орындауы керек:

- резиденттік антивирустық мониторинг;
- жаңа қауіптерден бұлтқа негізделген қорғаныс, бұл қолданбаға іске қосылып жатқан бағдарлама немесе файл туралы шешім алу үшін өндірушінің арнайы ресурстарына нақты уақыт режимінде қол жеткізуге мүмкіндік береді;
- SMB/NFS арқылы қолжетімді ресурстарды тексеру;
- ядро жадын тексеру мүмкіндігі;
- бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- пайдаланушы немесе әкімші командасы бойынша және кесте бойынша антивирустық сканерлеу;
- zip архивтеріндегі файлдарды антивирустық сканерлеу ; .7z*; .7-z; . rar ; . iso ; . такси ; . банка ; .bz;.bz2;. tbz ;.tbz 2; .gz;.tgz; . arj .;
- кіріс және шығыс электрондық пошта хабарламаларын тексеру;
- файлдарды сканерлеуді оңтайландыру механизмдерінің болуы (ерекшеліктері, сенімді процестер, сканерлеу уақытының шегі, сканерлеу файлының өлшемінің шегі, сканерленген және сканерлеуден кейін өзгертілмеген файлдар туралы ақпаратты кэштеу механизмі);
- SMB/NFS хаттамалары арқылы желіге кіру мүмкіндігі бар жергілікті каталогтардағы файлдарды қашықтағы зиянды шифрлаудан қорғау;
- сканерлеу кезінде файлдарды бұғаттау опциясын қосыңыз;

- күдікті және зақымдалған заттарды карантинге орналастыру;
- SAMBA деңгейінде файлдық операцияларды ұстап алу және тексеру;
- ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің брандмауэрін басқару;
- тапсырмаларды кесте бойынша және/немесе операциялық жүйені жүктегеннен кейін бірден іске қосу;
- есептерді HTML және CSV форматтарында экспорттау және сақтау;
- Файл кеңістігін сканерлеу кезінде пайдаланушының ыңғайлы тәжірибесін қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- егер ақпараттық құндылығы болса, нысанды сұраныс бойынша қалпына келтіру мүмкіндігі мақсатында өңдеу және жою алдында зарарланған нысанның көшірмесін резервтік сақтау орнында сақтау;
- түбірлік құқықтардысыз пайдаланушы графикалық интерфейсі арқылы басқару ;
- жоғарыда аталған барлық компоненттерді бірыңғай басқару жүйесін немесе веб-консольді пайдаланып орталықтандырылған басқару;
- құрылғы түрі және қосылым шинасы бойынша компьютерге орнатылған немесе қосылған құрылғыларға пайдаланушының кіруін басқару;
- алынбалы дискілерді тексеру;
- желілік шабуылдарға тән белсенділікті анықтау үшін кіріс желілік трафикті бақылау;
- пайдаланушының компьютеріне HTTP/HTTPS және FTP хаттамалары арқылы келетін трафикті тексеру, сондай-ақ веб-мекенжайлардың зиянды немесе фишингтік екенін анықтау мүмкіндігі
- пайдаланушының компьютеріндегі бағдарламалардың әрекеттері туралы деректер алу;
- компьютерлерде сақталған барлық орындалатын бағдарлама файлдары туралы ақпарат алу (Түгендеу тапсырмасы);
- бағдарлама басталған кезде іздеу файлдарын жасау;
- компьютерлерде орнатылған бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу;
- іске қосу нысандарын, жүктеу секторларын, процесс жадын және ядро жадын тексеру;
- өңдеу немесе жою алдында файлдардың сақтық көшірмелерін сақтау және сақтық көшірмелерден файлдарды қалпына келтіру;
- жалпы бағдарлама параметрлерінде процестерді жадты тексеруден алып тастау;
- SkipPlainTextFiles параметрін пайдаланып бағдарлама журналдарын тексеруді оңтайландыру ;
- бағдарламаны сканерлеуден трафикті алып тастау;
- JSON форматын сұраныстар мен ақпаратты шығару үшін, сондай-ақ бағдарлама параметрлері мен тапсырма параметрлерін экспорттау және импорттау үшін пайдаланыңыз;
- Arm архитектурасына арналған операциялық жүйелері бар құрылғыларда орнату және пайдалану ;
- қауіптер анықталған жағдайда немесе құрылғыға кіру әрекеті анықталған кезде пайдаланушыға хабарландыру режимінде жұмыс істеу;
- тыйым салынған немесе рұқсат етілген қолданба режимдерінің тізіміндегі басқару ережелерін пайдаланып, қорғалған құрылғыларда қолданбаларды іске қосуды басқару мүмкіндігі;

- Жаңарту кезінде қолданбаны автоматты түрде қайта іске қосу;
- процессор ресурстарын пайдалануға шектеулер қою мүмкіндігі;
- орнатудан кейін қолданбаны іске қосқан кезде қорғаныс компоненттерін және сканерлеу тапсырмаларын автоматты түрде өшіру мүмкіндігі;
- графикалық пайдаланушы интерфейсіндегі компоненттер мен тапсырмалардың жұмысы туралы пайдаланушыға хабарландырулар;
- процесс жадын тоқтатпай оқу мүмкіндігі (3.4 нұсқасынан бастап Linux ядролары);
- пайдаланушылардың веб-ресурстарға кіруін басқару мүмкіндігі;
- қорғалған құрылғыларда қолданбаларды іске қосуды басқару мүмкіндігі;
- қолданбаның өз жұмысының тұрақтылығын бақылау функциясы;
- сканерлеуден нысандарды алып тастауды конфигурациялау мүмкіндігімен эксплойттардан қорғау;
- қосылған құрылғыларға сенімді болатын құрылғыны басқару пайдаланушыларының немесе пайдаланушы топтарының тізімін конфигурациялау мүмкіндігі;
- сақтау құрылғыларына тек оқуға арналған қолжетімділікті қамтамасыз ету мүмкіндігі;
- прокси-серверді пайдаланған кезде жеке қолданба компоненттері үшін ерекше жағдайларды конфигурациялау мүмкіндігі;
- трафикті ұстап алудан ерекше жағдайларды конфигурациялау мүмкіндігі;
- дерекқор журнал файлдарын сканерлеуден уақытша алып тастау мүмкіндігі;
- қолданбаға қолданылатын саясаттар мен тапсырмалардағы ерекшеліктер тізімдерін экспорттау және импорттау мүмкіндігі;
- батарея қуатымен жұмыс істейтін құрылғыда жоспарланған тапсырмаларды болдырмауды конфигурациялау мүмкіндігі;
- пәрмен жолында қолданба функцияларының тізімін, олардың мәртебесі (пайдаланылған немесе пайдаланылмаған) және осы қолданба функцияларын іске асыру үшін қолданылатын Linux технологиялары туралы ақпаратты көрсету мүмкіндігі;
- BadUSB типті шабуылдардан қорғау мүмкіндігі ;
- құрылғыда қазіргі уақытта қолданылып жатқан саясат және саясат профильдері туралы ақпаратты пәрмен жолында және графикалық интерфейсте көрсету мүмкіндігі.

Мобильді құрылғыларға арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар

Смартфондарға арналған антивирустық бағдарламалық жасақтама келесі мобильді операциялық жүйелермен үйлесімді болуы керек:

1. Android 5.0 және одан жоғары нұсқалары (Android 12 L қоса алғанда , Go қоспағанда) Басылым);
2. iOS 15 және одан жоғары нұсқалары немесе iPadOS 15 және одан жоғары нұсқалары;

Android операциялық жүйесінде жұмыс істейтін смартфондарға арналған антивирустық қорғау бағдарламалық жасақтамасында келесі функциялар орындалуы керек :

- Смартфонның файлдық жүйесін үнемі антивирустық қорғау, антивирустық қорғау өндірушісінің бұлттық бедел қызметін пайдаланып қосымша тексеру деңгейімен;

- құрылғының файлдық жүйесін сұраныс бойынша және жоспарланған түрде тексеру;
- Орнатылған қолданбаларды лезде тексеру
- антивирустық бағдарламалық жасақтама өндірушісінің беделді бұлттық қызметтерінің шешімдеріне негізделген зиянды және фишингтік веб-сайттарды бұғаттау;
- жұқтырған нысандарды оқшаулауға арналған сақтау орнының болуы;
- зиянды бағдарламаларды іздеу және қауіпті нысандарды жоспарлы түрде жою үшін пайдаланылатын антивирустық дерекқорларды жаңарту;
- алдын ала анықталған қолданба санаттарын пайдалануды қоса алғанда, көрсетілген қолданбалардың іске қосылуын бұғаттау;
- рұқсат етілген қолданбаларды ақ тізімге қосуды қолдау;
- қолданбаны іске қосуды басқарудың бөлігі ретінде жүйелік қолданбаларды бұғаттау;
- Firebase қызметі арқылы командалар мен push хабарландыруларын жіберу Бұлт Хабарлама алмасу (FCM);
- Wi-Fi және Bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануды блоктау ;
- wi-Fi желілеріне қосылу параметрлерін көрсетіңіз ;
- орнатылуы керек қолданбаларды көрсетіңіз;
- мобильді құрылғыны бұғаттау, деректерді жою, жұмыс әрекеттеріне қатысты деректерді жою , құрылғының орналасқан жерінің координаттарын алу, зауыттық параметрлерге қашықтан қалпына келтіру (зауыттық) қалпына келтіру);
- сәйкессіздіктер анықталған жағдайда құрылғыны автоматты түрде бұғаттау, деректерді жою және корпоративтік қосымшаларды іске қосуға тыйым салу мүмкіндігімен мобильді құрылғының корпоративтік саясатқа сәйкестігі тексерілетін ережелер тізімін жасау ;
- Samsung KNOX1 және KNOX2 технологияларын қолдау;
- Android құрылғыларына арналған қолданбаны басқару ережелерін жасаған кезде рұқсат етілген қолданба нұсқаларын көрсетіңіз .

iOS операциялық жүйесіне арналған смартфондарды қорғау үшін бағдарламалық жасақтамада келесі функциялар іске асырылуы керек :

- топтық саясаттарды пайдаланып, iOS MDM құрылғысының параметрлерін қашықтан конфигурациялау ;
- деректерді бұғаттау және жою командасын жіберу;
- мобильді құрылғыларға арналған топтық қауіпсіздік саясатын жасау;
- Exchange ActiveSync \ iOS MDM хаттамасы арқылы қосылған құрылғылардың конфигурация параметрлерін қашықтан конфигурациялау;
- пайдаланушылардың мобильді құрылғыларының жұмысы туралы есептер мен статистика алу;
- Бақыланатын антивирустық қорғауды жеткізушінің беделді бұлттық қызметтерінің шешімдеріне негізделген зиянды және фишингтік сайттарды бұғаттау режим ;
- бірыңғай басқару консолін пайдалана отырып, орталықтандырылған басқару;
- iTunes , Safari немесе Game Center сияқты жергілікті құрылғы қолданбаларын басқарылатын құрылғыда пайдалануға болатынын басқаруға мүмкіндік беретін компоненттің болуы .

- iOS MDM құрылғылары үшін Bluetooth параметрлеріне енгізілген өзгерістерді өшіру .

Веб-трафикті қорғау жүйесіне қойылатын талаптар

Жүйе формада берілуі керек

- Алдын ала орнатылған операциялық жүйе, прокси-сервер және трафик қауіпсіздігі мен басқару құралдары бар ISO кескіні
- Трафикті қорғау және басқару бағдарламасының дистрибуциясын қамтитын RPM немесе DEB пакеті

Жүйе келесі операциялық жүйелерде орнатуды және жұмыс істеуді қолдауы керек:

- CentOS 7.7.
- Rocky Linux 8.10, 9.4.
- Red Hat Enterprise Linux 7.7, 8.10, 9.4 нұсқалары .
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS.
- Debian 9.13, 10.13, 11.10, 12.10.
- SUSE Linux Enterprise Server 15 SP1.
- ҚЫЗЫЛ ОС 7.3, 8.0.
- Балама сервер 10.

Жүйе физикалық және виртуалды серверде орнатуды қолдауы керек; виртуалды ортада жұмыс істеу үшін ол келесі гипервизорларда орнатуды қолдауы керек:

- VMware ESXi 6.7 жаңартуы 3.
- VMware ESXi 7.0 жаңартуы 3.
- VMware ESXi 8.0 жаңартуы 3.
- Microsoft Hyper-V сервері 2019.
- Hyper-V рөлі орнатылған Windows Server 2019 Standard.
- Hyper-V рөлі орнатылған Windows Server 2022 Standard.
- ED виртуализациясы 7.3

Веб-трафикті қорғау жүйесі веб-ресурстармен жұмыс істеген кезде корпоративтік желі пайдаланушыларын қорғауды қамтамасыз етуі керек: HTTP(S) және FTP хаттамалары арқылы Интернеттен корпоративтік желіге келетін деректер ағынынан қауіп төндіретін зиянды бағдарламалар мен басқа да бағдарламаларды жою, зарарланған және фишингтік веб-сайттарды бұғаттау және веб-ресурстардың санаттары мен мазмұн түрлеріне негізделген веб-ресурстарға кіруді бақылау және келесі функцияларды қамтамасыз ету:

- Прокси-сервер арқылы берілетін нысандарды антивирустық сканерлеуді орындаңыз.
- анықталған жұқтырған нысандарды емдеу және емдеу мүмкін болмаған жағдайда, нысанға кіруге тыйым салу.
- Барлық файлдар мен қосымшалардағы вирустарды анықтаңыз және емдеңіз.
- Зиянды және фишингтік веб-сайттарды бұғаттау.
- Бағдарлама дерекқорының жаңартуларын күтпей-ақ қауіптерге жылдам жауап беруді қамтамасыз ету, сондай-ақ жалған оң нәтижелердің ықтималдығын азайту үшін

антивирустық бағдарлама жеткізушісінің беделіне негізделген бұлттық қызметтеріне негізделген қосымша тексеру деңгейін пайдаланыңыз.

- Кірістірілген немесе сыртқы прокси-сервердегі сертификатты ауыстырған кезде SSL шифрланған желілік трафикті бақылаңыз және қорғаңыз.
- келесі критерийлерге негізделген кіру және қорғау ережелерін конфигурациялаңыз:
    1. Веб-сайт санаты
    2. Ресурс URL мекенжайы
    3. Файл атауы
    4. Файл түрі
    5. Файл өлшемі
    6. MIME түрі
    7. Файлдың хэш қосындысы (MD 5, SHA 256)
    8. Жол қозғалысы бағыты
    9. HTTP әдісі
    10. HTTP мазмұнының ұзындығы
    11. LDAP жазбасы
    12. Пайдаланушы-агент
    13. IP мекенжайы немесе ішкі желі маскасы
- кіру құқықтары мен қорғаудың басымдығын конфигурациялау
- қауіпсіздік бағдарламалық жасақтамасын өндіруші анықтаған веб-сайт санаттары мен мазмұн түрлеріне негізделген пайдаланушылардың интернет ресурстарына кіруін басқару.
- URL маскалары мен тұрақты өрнектерді сүзгі ретінде қолдау.
- пайдаланушылардың тек белгілі бір веб-шолғыш түрін пайдалануын бақылау (басқарылатын ұйымдарда браузер клиенттерін бұғаттауға тыйым салынады).
- пайдаланушының интернет ресурстарына кіруін басқару ережелерінің уақытша кестесін конфигурациялау.
- Басқару консолі пайдаланушыларына рөлдерді тағайындау үшін Microsoft Active Directory-мен интеграциялаңыз.
- бірнеше Microsoft Active Directory домендерімен интеграциялау мүмкіндігін қамтамасыз етеді.
- Бірыңғай кіру қызметі үшін NTLM және Kerberos аутентификациясын қолдауды қамтамасыз етеді .
- Р жазбаларына негізделген арнайы топтарға арналған жұмыс кеңістіктерін қолдауды қамтамасыз етіңіз .
- Жұмыс кеңістіктері үшін жеке трафикті өңдеу және тексеру ережелерін, сондай-ақ осы ұйымдардың әкімшілерінің кіру құқықтарын конфигурациялаңыз.
- әрбір жұмыс кеңістігі үшін құлыптау бетінің көрінісін бөлек реттеу мүмкіндігі
- пайдаланушыға интернет-ресурстың бұғатталғаны туралы хабарлай отырып, веб-беттің сыртқы түрін реттеу.
- статистиканы, соның ішінде антивирустық сканерлеудің орындалуы мен нәтижелері, қолданба қателері және ескертулер туралы ақпаратты жүргізу.
- Бағдарлама оқиғалары журналдарын CSV форматында экспорттауға мүмкіндік береді.
- Оқиғаларды іздеу және шолу арқылы интернетке кіру оқиғаларын зерттеңіз.
- Іс-шара картасында, басқалармен қатар, мыналар болуы керек:

1. URL мекенжайы
2. хаттама
3. домен
4. қауіпсіздік технологиялары арқылы анықтау нәтижесі
5. оқиғаның болған уақыты
6. пайдаланушы аты
7. Пайдаланушы агенті
8. IP мекенжайы
9. веб-ресурс тиесілі санат

- Syslog хаттамасы арқылы қауіпсіздік туралы ақпарат және оқиғаларды басқару жүйесіне (SIEM) жариялаңыз . Әрбір оқиға туралы ақпарат CEF форматында бөлек Syslog хабарламасы ретінде берілуі керек .
- веб-интерфейс арқылы бағдарлама туралы диагностикалық ақпаратты жинау мүмкіндігін қамтамасыз ету
- бағдарлама параметрлерін конфигурациялау және веб-интерфейс арқылы бағдарламаны басқару
- бағдарлама параметрлерінің мәндерін импорттау және экспорттау мүмкіндігін қолдау
- SNMP хаттамасы арқылы бағдарламаның жұмыс статистикасын алу, SNMP тұзақтарын жіберуді қосу және өшіру
- веб- интерфейсі арқылы бағдарламаның жұмыс күйін, бағдарлама өңдеген желілік трафикті, сканерленген және анықталған нысандар санын, соңғы және ең жиі кездесетін қауіптерді, бұғатталған пайдаланушыларды және URL мекенжайларын бақылаңыз .
- антивирустық дерекқорларды өндірушінің веб-сайтынан (қауіпсіз және қорғалмаған H TTP протоколы арқылы) және конфигурацияланатын ресурстардан (HTTP және FTP серверлері) кесте бойынша немесе сұраныс бойынша жаңартыңыз.
- бағдарламаның веб-интерфейсі арқылы прокси-сервер параметрлерін конфигурациялау (ISO файлынан орналастырған кезде)
- жасалған кіру және қорғау ережелерін топтастыру мүмкіндігі
- қауіпсіздік және кіруді бақылау механизмдері арқылы өңдеуді қажет етпейтін веб-ресурстар үшін айналып өту ережелерін жасау
- әдепкі қорғау ережелерін орнату мүмкіндігі
- бағдарламаның веб-интерфейсі арқылы кіріктірілген прокси-серверді басқару мүмкіндігі
- PROXY протоколын және HTTP бағытталған тақырыптарын қолдау арқылы сенімді жүктеме теңгергіштерін қосу
- Kerberos және NTLM арқылы прокси-серверде пайдаланушыларды аутентификациялау
- өздігінен қол қойылған немесе корпоративтік сертификатты пайдаланып HTTPS трафи гін шифрдан шығару мүмкіндігі
- трафикті шифрлау ережелерін жасау мүмкіндігі, соның ішінде IP және домен атаулары бойынша ресурстарды шифрлау ережелерінен алып тастау
- сенімді сертификаттардың саусақ іздерін жүйенің жадына қосу мүмкіндігі
- прокси-сервер журналының сақтау форматын басқару мүмкіндігі
- шешімді кластерлеу мүмкіндігі

- кластерге жиналған жүйелік серверлерді орталықтан басқару және бақылау мүмкіндігі
- Веб-трафикті қорғау жүйесі алған файлдарды талдау үшін жіберу, сондай-ақ сканерлеу нәтижелерін алу үшін құмсалғыш типті жүйелермен интеграциялау мүмкіндігін қолдау қажет.
- PDF форматында жасау мүмкіндігі .

Бөлек серверді пайдаланатын антивирустық қорғаныс және спамды сүзу бағдарламалық жасақтамасына қойылатын талаптар

Жүйе келесі түрде жеткізіледі:

1. Rocky Linux 9.8 операциялық жүйесіне негізделген алдын ала орнатылған операциялық жүйе, пошта сервері және пошта трафигін қорғау құралдары бар ISO кескіні . Rocky Linux 9.8 операциялық жүйесі жүйе кескініне кіреді.
2. redos-8-20250711.7-Everything-x86_64-DVD1.iso файлынан алынған RED OS 8.0 операциялық жүйесіне негізделген алдын ала орнатылған операциялық жүйе, пошта сервері және пошта трафигін қорғау құралдары бар ISO кескіні .

-

Жүйе физикалық және виртуалды серверде орнатуды қолдауы керек; виртуалды ортада жұмыс істеу үшін ол келесі гипервизорларда орнатуды қолдауы керек:

1. VMware ESXi 7.0 жаңартуы 3;
2. VMware ESXi 8.0 жаңартуы 3;
3. Microsoft Hyper-V Server 2019;
4. Microsoft Hyper-V Server 2022;
5. Windows Server 2019 стандартымен Гипер-V рөлі ;
6. Windows Server 2022 Standard бағдарламасымен Гипер-V рөлі ;
7. ED виртуалдандыруы 7.3.0;
8. ED виртуалдандыруы 7.3.3;
9. VMmanager 2026.01.1-1 жүйесінде жұмыс істейтін Astra Linux Special Edition 1.8.3 негізіндегі гипервизор

Антивирустық қорғау және спамды сүзу бағдарламалық жасақтамасы келесі функцияларды қамтамасыз етуі керек:

- кіріс және шығыс электрондық пошта хабарламалары ағынындағы, соның ішінде қосымшалардағы барлық вирус түрлерін, құрттарды, трояндарды және басқа да зиянды бағдарламаларды нақты уақыт режимінде іздеу және жою;
- кіріс электрондық пошта ағынын спамға, ықтимал спамға, жаппай пошта жіберулерге (соның ішінде маркетингтік пошта жіберулерге) тексеру, анықталған хабарламаларды жою, хабарламалардың көшірмесін карантинге қою;
- жалпы хабарлама карантинінің болуы ;
- веб-интерфейс арқылы карантинді басқару;

- электрондық поштаның негізгі бөлігіндегі зиянды және фишингтік сілтемелерді, соның ішінде кескін қосымшаларындағы QR кодтарынан алынған сілтемелерді анықтау;
- эвристикалық анықтау әдістерінің болуы;
- хабарламаның басына және хабарламаның MIME бөлігіне ақпараттық тақырыптарды қосуды қосу немесе өшіру мүмкіндігі;
- хабарлама алушыларды қолмен толтырылған немесе LDAP-пен интеграциялау арқылы қабылданатын алушылар тізімімен салыстыру мүмкіндігі;
- қолданба параметрлерін шифрланған түрде экспорттау мүмкіндігі;
- өнімнің веб-интерфейсінде хабарлама мазмұнын көру мүмкіндігі;
- беделді бұлттық қызметтерді пайдалану мүмкіндігі;
- ұйымнан тыс деректерді жібермей тексеруге мүмкіндік беретін жеке бедел қызметімен интеграциялау мүмкіндігі;
- қауіптерді блоктау үшін күрделі файлдарды ауытқуларға ашу және талдауға мүмкіндік беретін қауіпсіздік компонентінің болуы;
- жұқтырған электрондық пошта хабарламалары мен жұқтырған қосымшаларды анықтау, блоктау және зарарсыздандыру, хабарламалар мен қосымшаларды жою және хабарламалардың көшірмелерін карантинге қою;
- тіркемелерде макростар бар хабарламаларды анықтау және бұғаттау (мысалы, макростары бар Microsoft Office форматындағы файлдар), хабарламаларды немесе тіркемелерді жою және хабарламалардың көшірмелерін карантинге қою;
- шифрланған нысандары бар хабарламаларды анықтау және бұғаттау, хабарламаларды немесе қосымшаларды жою және хабарламалардың көшірмелерін карантинге қою;
- мұрағаттар бар хабарламаларды анықтау және бұғаттау, мұрағаттардағы файл түрлерін тану, жеке файлдарды бұғаттау;
- хабарламалардың мазмұнын атауы (мұрағаттар мен құрама нысандарды қоса алғанда), қосымшалардың өлшемі мен түрі, тақырыптары, тақырыбы және негізгі мәтіні бойынша сүзгілеуді жүзеге асыру, кеңейтілуіне қарамастан қосымшаның форматы мен түрін анықтау, белгілі бір форматтағы немесе белгілі бір атаудағы қосымшалары бар хабарламаларды немесе өлшемі рұқсат етілген шектен асатын хабарламаларды жою, хабарламалардың көшірмелерін сақтау орнына орналастыру;
- қорғаныс модульдерінің өңдеу нәтижелеріне негізделген карантиндегі хабарламалардың сақтық көшірмелерін сақтау;
- карантиндегі хабарламаларды файлға сақтау және хабарламаларды алушыларға жіберу;
- орталықтандырылған басқаруы бар кластер архитектурасын орналастыруды қолдау және кіріс пошта трафигін бірнеше серверлер арасында басымдық параметрлерімен жаһандық деңгейде де, жеке домендер үшін де теңестіру мүмкіндігі;
- Active Directory каталог қызметтерімен интеграция, соның ішінде көп деңгейлі Active Directory ормандарын (орман кеңістігі), ALD Pro қолдауы;−
- SNMP арқылы тұзақтарды жіберу мүмкіндігі, соның ішінде спам карантиніне, мақсатты шабуыл карантиніне және сканерлеу статистикасына арналған кеңейтілген есептегіштер (анықталған/анықталмаған қауіптер санын, сканерлеу қателерін және тайм-ауттарды қоса алғанда);

- электрондық пошта хабарламаларын жіберушілер мен алушылар топтары үшін белгіленген ережелерге сәйкес өңдеу;
- ережелерді клондау және оларды тізімге сүйреп апару арқылы басымдықты өзгерту мүмкіндігі;
- Ережелерді орнатқан кезде, хабарламаға тек іске қосылатын ереженің нәтижесіне ғана емес, сонымен қатар әрбір қауіпсіздік модулінің бөлек іске қосылу нәтижесіне де негізделіп ескертпелер қосу мүмкіндігі болуы керек;
- пайдаланушыларға бағдарлама модульдері арқылы олардың хабарламаларын тексеру нәтижелері туралы хабарламалар жіберу;
- LDAP жазбаларына негізделген жеке карантиннің жұмысын қолдау ;
- LDAP тіркелгілеріне негізделуі керек ;
- Жеке карантиннің мәртебесі туралы пайдаланушыларға хабарландырулар жіберу; хабарландыруларда карантиндегі соңғы хабарламалардың тізімі болуы керек;
- хабарландыру жіберу кестесінің параметрлері;
- пайдаланушының жеке жадында орналастырылған соңғы хабарламалар туралы ақпараты бар электрондық пошталарды жіберу мүмкіндігі, жеке жадтан да, электрондық пошта хабарламасынан да хабарламалармен рұқсат етілген әрекеттерді орындау мүмкіндігі;
- электрондық пошта хабарламаларын сақтау орнынан жібермес бұрын қауіпсіздік технологиялары арқылы қайта тексеруге болатынына көз жеткізіңіз;
- хабарламаның негізгі бөлігіндегі шифрланған қосымшаларды автоматты түрде құпия сөзбен іздеуді қолдау;
- электрондық пошта хабарламасының мәтінінде құпия сөздерді автоматты түрде іздеу және оларды қосымшаларда қамтылған құпия сөзбен қорғалған Microsoft Office құжаттарын тексеру үшін пайдалану мүмкіндігін қамтамасыз ету;
- бағдарлама дерекқорларын жаңарту серверлерінен және пайдаланушы ресурстарынан (HTTP, HTTPS және FTP серверлері, жергілікті және желілік қалталар) кестеге сәйкес және сұраныс бойынша жаңарту;
- қауіпсіз TLS/SSL арнасы арқылы хабарламалар жіберу және қабылдау, шифрлау кілттерін басқару;
- жүйе басқа серверден хабарламалар алатын (сервер ретінде әрекет ететін) немесе хабарламаларды басқа серверге жіберетін (клиент ретінде әрекет ететін) жағдайлар үшін TLS хабарламаларын шифрлау режимдерін конфигурациялау және жеке домендер үшін TLS параметрлерін конфигурациялау;
- SPF, DKIM және DMARC технологияларын пайдаланып хабарлама жіберушінің аутентификациясын орындаңыз, әрбір технология сүзгі өрнектерінде бөлек шарт ретінде конфигурациялануы мүмкін;
- DKIM технологиясын пайдаланып шығыс электрондық пошта хабарламаларына қол қою;
- әрбір SPF және DMARC тексеру күйі үшін хабарламаға бөлек әрекет орнату және әрбір тексеру нәтижелеріне негізделген хабарландыруларды конфигурациялау мүмкіндігі;
- жіберуші доменін сәйкестендіру технологиясын пайдаланып, хабарлама жіберушілердің түпнұсқалығын тексеру;

- веб-интерфейс арқылы конфигурациясы бар SIEM жүйесіне оқиғаларды жариялау мүмкіндігі;
- Тақырып жолына кіріс хабарламаларға қауіпті тіркемелер туралы ескертулерді қосыңыз;
- оқиға журналын қараңыз, бағдарламаның веб-интерфейсінде аудит жүргізіңіз және оны қатты дискіңізге жүктеңіз;
- өзіңіздің «қара» және «ақ» тізімдеріңізге негізделген жіберушінің мекенжайы (электрондық пошта және/немесе IP мекенжайы) бойынша хабарламаларды сүзу немесе сүзгіден шығару;
- SMTP сеансында (MAIL FROM командасының мәні) және хабарламада (From MIME тақырыбының мәні) көрсетілген хабарламаның жіберуші домендерінің сәйкестігін тексеру;
- SMTP сеансында жіберуші мен алушы мекенжайларының синтаксисінің дұрыстығын RFC стандартына сәйкестігін тексеру;
- сурет қосымшаларын белгілі спам хабарлама қолтаңбаларымен сәйкестікке тексеру;
- күдікті, зақымдалған және құпия сөзбен қорғалған файлдарды, сондай-ақ сканерлеу сәтсіз аяқталған файлдарды анықтау;
- жұқтырған, күдікті және зақымдалған пошта трафигі нысандарын карантинге ауыстыру, құпия сөзбен қорғалған файлдарды, сондай-ақ сканерлеуден өтпеген файлдарды анықтау;
- сүзу ережелерін жасаған кезде тұрақты өрнектерді пайдалану;
- Электрондық поштаны сүзу ережелерінде Microsoft Active Directory каталогынан пайдаланушылар мен пайдаланушы топтарын көрсетіңіз;
- кіріктірілген әкімші және қолдау маманы рөлдерінің болуы;
- жіберушіге, алушыға және сервер әкімшісіне жұқтырылған және күдікті нысандары бар электрондық пошта хабарламасы туралы хабарлау мүмкіндігі;
- Бағдарламаны командалық жолды пайдаланып, стандартты операциялық жүйе құралдарымен де, келесі браузерлерде жұмыс істейтін арнайы веб-интерфейс арқылы да басқару керек: Mozilla Firefox 127.0.2 немесе одан жоғары нұсқасы, Google Chrome 129.0.6668 немесе одан жоғары нұсқасы, Microsoft Edge 129.0.2792 немесе одан жоғары нұсқасы;
- Файлдарды талдау үшін жіберуге арналған құм жәшігі типті жүйелермен интеграциялау мүмкіндігі қолдау табуы керек, әрбір хабарламаға бірегей идентификатор (UUID) тағайындалады, сондай-ақ құм жәшігіне жіберілген әрбір модуль үшін алушылардың тізімі мен тексеру нәтижелері көрсетіледі;
- PDF форматында жасау мүмкіндігі ;
- Юникод спуфингімен хабарларды анықтаңыз. Егер Юникод спуфингісі анықталса, хабарды спам деп есептеңіз.
- пошта трафигін веб-интерфейс арқылы бағыттауды басқару мүмкіндігі, оның ішінде пошта хабарламаларын тақырыптарының атауы мен мәніне қарай бағыттау;
- Виртуалды машинаны орналастырғаннан кейін MTA және желі параметрлерін жылдам конфигурациялау үшін бастапқы орнату шебері қолжетімді болуы керек;

- Жүйе басқа серверден хабарламалар алатын (сервер ретінде әрекет ететін) немесе хабарламаларды басқа серверге жіберетін (клиент ретінде әрекет ететін) жағдайлар үшін TLS хабарламаларын шифрлау режимдерін конфигурациялаңыз және жеке домендер үшін TLS параметрлерін конфигурациялаңыз.
- шабуыл жасау мақсатында әдейі өзгертілген немесе бағдарламалық жасақтама қателеріне байланысты дұрыс емес құрылған хабарламаларды қоса алғанда, құрылымы бұзылған немесе дұрыс емес электрондық пошта хабарламаларын анықтау, мұндай хабарламалар бойынша әрекеттерді реттеу мүмкіндігімен;
- қызметтік тақырыптардағы электрондық пошта хабарламасының бағыты туралы техникалық ақпаратты ескере отырып, жіберушілердің IP мекенжайлары мен домендерінің беделін тексеруді жүргізу;
- электрондық пошта хабарламаларын өңдеу ережелері қолданылғанға дейін көрсетілген тақырыптарды орталықтандырылған түрде алып тастау мүмкіндігін қамтамасыз ету;
- электрондық пошта хабарламаларын олардың параметрлеріне негізделген өңдеу ережелерін іздеу және сүзу мүмкіндігін қамтамасыз ету, сондай-ақ ережелерде пайдаланылған жіберушілер мен алушылардың тізімдеріне түсініктемелер қосу;
- жүйелік журналдарды тікелей веб-интерфейс арқылы қарау;
- хабарламаның 10 MIME бөлігіне дейінгі талдауды қоса алғанда, мазмұнды сүзу ережелерін іске қосу туралы егжей-тегжейлі ақпаратты тіркеу;
- Бағдарлама MTA, маршруттау, DKIM және TLS кілттерін, домендерді және мекенжайларды конфигурациялауға мүмкіндік беретін веб-интерфейс арқылы басқарылуы керек;
- белгілі бір уақыт аралығында зиянды, фишингтік және спам мазмұны бар хабарламаларды қоса алғанда, қауіпті электрондық пошта хабарламаларын жиі алған пайдаланушылар туралы статистикалық ақпаратты жасауды және көрсетуді қамтамасыз ету;
- электрондық пошта хабарламасының мәтініндегі құпия сөздерді автоматты түрде анықтау және оларды қосымшаларда қамтылған құпия сөзбен қорғалған Microsoft Office құжаттарын тексеру үшін пайдалану мүмкіндігін қамтамасыз ету.

Linux операциялық жүйелерінде орнатылған пошта серверлеріне арналған антивирустық қорғаныс және спамды сүзу бағдарламалық жасақтамасына қойылатын талаптар

Linux пошта серверлеріне арналған антивирустық және спам сүзгілеу бағдарламалық жасақтамасы келесі 64 биттік операциялық жүйелерді іске қосатын компьютерлерде жұмыс істеуі керек:

1. Rocky Linux 9.7, 10.1;
2. Ubuntu 22.04 LTS, 24.04 LTS;
3. Red Hat Enterprise Linux 9.7, 10.1;
4. Debian 12.13, 13.3;

5. ҚЫЗЫЛ ОС 7.3 (тек -дан image redos-MUROM-7.3-20241221.0-Барлығы-x86_64-DVD1.iso);
6. ҚЫЗЫЛ OS 8.0 (тек redos-8-20250711.7-Everything-x86_64-DVD1.iso кескінінен алынған);
7. Астра Linux Арнайы 1.7 басылымы (Смоленск қауіпсіздік деңгейі), 1.7.9 жаңартуымен, БЮЛЛЕТЕНЬ №2025-1202 SE 17, жалпы ядро ;
8. Астра Linux Арнайы 1.8 басылымы (Смоленск қауіпсіздік деңгейі), 1.8.4 жаңартуымен, БЮЛЛЕТЕНЬ №2025-1113 SE 18, жалпы ядро ;

Linux пошта серверлеріне арналған антивирустық және спам сүзгілеу бағдарламалық жасақтамасы келесі пошта жүйесінің нұсқаларымен жұмыс істеуі керек:

1. Exim- 4.92 және одан жоғары .
2. Постфикс - 3.5.25 және одан жоғары .

Nginx веб-серверінің 1.18.1 немесе одан жоғары нұсқасымен бірге жұмыс істеуі керек . Astra Linux Special Edition жүйесін іске қосқан кезде Apache веб-серверінің 2.4.62 нұсқасы қажет.

Антивирустық қорғау және спамды сүзу бағдарламалық жасақтамасы келесі функцияларды қамтамасыз етуі керек:

- кіріс және шығыс электрондық пошта хабарламалары ағынындағы, соның ішінде қосымшалардағы барлық вирус түрлерін, құрттарды, трояндарды және басқа да зиянды бағдарламаларды нақты уақыт режимінде іздеу және жою;
- кіріс электрондық пошта ағынын спамға, ықтимал спамға, жаппай пошта жіберулерге (соның ішінде маркетингтік пошта жіберулерге) тексеру, анықталған хабарламаларды жою, хабарламалардың көшірмесін карантинге қою;
- жалпы хабарлама карантинінің болуы ;
- веб-интерфейс арқылы карантинді басқару;
- электрондық поштаның негізгі бөлігіндегі зиянды және фишингтік сілтемелерді, соның ішінде кескін қосымшаларындағы QR кодтарынан алынған сілтемелерді анықтау;
- эвристикалық анықтау әдістерінің болуы;
- хабарламаның басына және хабарламаның MIME бөлігіне ақпараттық тақырыптарды қосуды қосу немесе өшіру мүмкіндігі;
- хабарлама алушыларды қолмен толтырылған немесе LDAP-пен интеграциялау арқылы қабылданатын алушылар тізімімен салыстыру мүмкіндігі;
- қолданба параметрлерін шифрланған түрде экспорттау мүмкіндігі;
- өнімнің веб-интерфейсінде хабарлама мазмұнын көру мүмкіндігі;
- беделді бұлттық қызметтерді пайдалану мүмкіндігі;
- ұйымнан тыс деректерді жібермей тексеруге мүмкіндік беретін жеке бедел қызметімен интеграциялау мүмкіндігі;
- қауіптерді блоктау үшін күрделі файлдарды ауыткуларға ашу және талдауға мүмкіндік беретін қауіпсіздік компонентінің болуы;

- жұқтырған электрондық пошта хабарламалары мен жұқтырған қосымшаларды анықтау, блоктау және зарарсыздандыру, хабарламалар мен қосымшаларды жою және хабарламалардың көшірмелерін карантинге қою;
- тіркемелерде макростар бар хабарламаларды анықтау және бұғаттау (мысалы, макростары бар Microsoft Office форматындағы файлдар), хабарламаларды немесе тіркемелерді жою және хабарламалардың көшірмелерін карантинге қою;
- шифрланған нысандары бар хабарламаларды анықтау және бұғаттау, хабарламаларды немесе қосымшаларды жою және хабарламалардың көшірмелерін карантинге қою;
- мұрағаттар бар хабарламаларды анықтау және бұғаттау, мұрағаттардағы файл түрлерін тану, жеке файлдарды бұғаттау;
- хабарламалардың мазмұнын атауы (мұрағаттар мен құрама нысандарды қоса алғанда), тіркемелердің өлшемі мен түрі, тақырыптары, тақырыбы және негізгі мәтіні бойынша сүзгілеуді жүзеге асыру, кеңейтілуіне қарамастан тіркеменің форматы мен түрін анықтау, белгілі бір форматтағы немесе белгілі бір атаудағы тіркемелері бар хабарламаларды немесе өлшемі рұқсат етілген шектен асатын хабарламаларды жою, хабарламалардың көшірмелерін сақтау орнына орналастыру;
- қорғаныс модульдерінің өңдеу нәтижелеріне негізделген карантиндегі хабарламалардың сақтық көшірмелерін сақтау;
- карантиндегі хабарламаларды файлға сақтау және хабарламаларды алушыларға жіберу;
- Active Directory каталог қызметтерімен интеграция, соның ішінде көп деңгейлі Active Directory ормандарын (орман кеңістігі), ALD қолдауы Про ;
- SNMP арқылы тұзақтарды жіберу мүмкіндігі, соның ішінде спам карантиніне, мақсатты шабуыл карантиніне және сканерлеу статистикасына арналған кеңейтілген есептегіштер (анықталған/анықталмаған қауіптер санын, сканерлеу қателерін және тайм-ауттарды қоса алғанда);
- электрондық пошта хабарламаларын жіберушілер мен алушылар топтары үшін белгіленген ережелерге сәйкес өңдеу;
- пайдаланушыларға бағдарлама модульдері арқылы олардың хабарламаларын тексеру нәтижелері туралы хабарламалар жіберу;
- LDAP жазбаларына негізделген жеке карантиннің жұмысын қолдау ;
- LDAP тіркелгілеріне негізделуі керек ;
- пайдаланушыларға жеке карантиннің мәртебесі туралы хабарландырулар жіберу; хабарландыруларда карантиндегі соңғы хабарламалардың тізімі болуы керек;
- хабарландыру жіберу кестесінің параметрлері;
- пайдаланушының жеке жадында орналастырылған соңғы хабарламалар туралы ақпараты бар электрондық пошталарды жіберу мүмкіндігі, жеке жадтан да, электрондық пошта хабарламасынан да хабарламалармен рұқсат етілген әрекеттерді орындау мүмкіндігі;
- электрондық пошта хабарламаларын сақтау орнынан жібермес бұрын қауіпсіздік технологиялары арқылы қайта тексеруге болатынына көз жеткізіңіз;
- пайдаланушыға хабарламаларды қайта тексеру кезінде көрсетілген құпия сөздерді пайдалану үшін жеке сақтау орнынан электрондық пошта хабарламаларын жіберген кезде шифрланған нысандарға арналған құпия сөздерді енгізу мүмкіндігін қамтамасыз ету;

- хабарламаның негізгі бөлігіндегі шифрланған қосымшаларды автоматты түрде құпия сөзбен іздеуді қолдау;
- электрондық пошта хабарламасының мәтінінде құпия сөздерді автоматты түрде іздеу және оларды қосымшаларда қамтылған құпия сөзбен қорғалған Microsoft Office құжаттарын тексеру үшін пайдалану мүмкіндігін қамтамасыз ету;
- бағдарлама дерекқорларын жаңарту серверлерінен және пайдаланушы ресурстарынан (HTTP, HTTPS және FTP серверлері, жергілікті және желілік қалталар) кестеге сәйкес және сұраныс бойынша жаңарту;
- қауіпсіз TLS/SSL арнасы арқылы хабарламалар жіберу және қабылдау, шифрлау кілттерін басқару;
- жүйе басқа серверден хабарламалар алатын (сервер ретінде әрекет ететін) немесе хабарламаларды басқа серверге жіберетін (клиент ретінде әрекет ететін) жағдайлар үшін TLS хабарламаларын шифрлау режимдерін конфигурациялау және жеке домендер үшін TLS параметрлерін конфигурациялау;
- SPF, DKIM және DMARC технологияларын пайдаланып хабарлама жіберушінің аутентификациясын орындаңыз, әрбір технология сүзгі өрнектерінде бөлек шарт ретінде конфигурациялануы мүмкін;
- DKIM технологиясын пайдаланып шығыс электрондық пошта хабарламаларына қол қою;
- Тақырып жолына кіріс хабарламаларға қауіпті тіркемелер туралы ескертулерді қосыңыз;
- бағдарламаның веб-интерфейсінде оқиға мен аудит журналын қарап, оны қатты дискіңізге жүктеңіз;
- жүйелік журналдарды тікелей веб-интерфейс арқылы қарау;
- хабарламаның 10 MIME бөлігіне дейінгі талдауды қоса алғанда, мазмұнды сүзу ережелерін іске қосу туралы егжей-тегжейлі ақпаратты тіркеу;
- өзіңіздің «қара» және «ақ» тізімдеріңізге негізделген жіберушінің мекенжайы (электрондық пошта және/немесе IP мекенжайы) бойынша хабарламаларды сүзу немесе сүзгіден шығару;
- SMTP сеансында (MAIL FROM командасының мәні) және хабарламада (From MIME тақырыбының мәні) көрсетілген хабарламаның жіберуші домендерінің сәйкестігін тексеру;
- SMTP сеансында жіберуші мен алушы мекенжайларының синтаксисінің дұрыстығын RFC стандартына сәйкестігін тексеру;
- сурет қосымшаларын белгілі спам хабарлама қолтаңбаларымен сәйкестікке тексеру;
- күдікті, зақымдалған және құпия сөзбен қорғалған файлдарды, сондай-ақ сканерлеу сәтсіз аяқталған файлдарды анықтау;
- жұқтырған, күдікті және зақымдалған пошта трафигі нысандарын карантинге ауыстыру, құпия сөзбен қорғалған файлдарды, сондай-ақ сканерлеуден өтпеген файлдарды анықтау;
- сүзу ережелерін жасаған кезде тұрақты өрнектерді пайдалану;
- Электрондық поштаны сүзу ережелерінде Microsoft Active Directory каталогынан пайдаланушылар мен пайдаланушы топтарын көрсетіңіз;
- кіріктірілген әкімші және қолдау маманы рөлдерінің болуы;

- жіберушіге, алушыға және сервер әкімшісіне жұқтырылған және күдікті нысандары бар электрондық пошта хабарламасы туралы хабарлау мүмкіндігі;
- бағдарламаның жұмысын командалық жолды пайдаланып стандартты операциялық жүйе құралдарымен де, келесі браузерлерде жұмыс істейтін арнайы веб-интерфейс арқылы да басқару керек: Mozilla Firefox 127.0.2 немесе одан жоғары нұсқасы, Google Chrome 139.0.7258 немесе одан жоғары нұсқасы, Microsoft Edge 139.0.3405 немесе одан жоғары нұсқасы;
- Файлдарды талдау үшін жіберуге арналған құм жәшігі типті жүйелермен интеграциялау мүмкіндігі қолдау көрсетілуі керек, әрбір хабарламаға бірегей идентификатор (UUID) тағайындалады, сондай-ақ құм жәшігіне жіберілген әрбір модуль үшін алушылардың тізімі мен тексеру нәтижелері көрсетіледі;
- PDF форматында жасау мүмкіндігі ;
- Юникод спуфингімен хабарларды анықтайды. Егер Юникод спуфингісі анықталса, хабар спам болып саналады.
- шабуыл жасау мақсатында әдейі өзгертілген немесе бағдарламалық жасақтама қателеріне байланысты дұрыс емес құрылған хабарламаларды қоса алғанда, құрылымы бұзылған немесе дұрыс емес электрондық пошта хабарламаларын анықтау, мұндай хабарламалар бойынша әрекеттерді реттеу мүмкіндігімен;
- қызметтік тақырыптардағы электрондық пошта хабарламасының бағыты туралы техникалық ақпаратты ескере отырып, жіберушілердің IP мекенжайлары мен домендерінің беделін тексеруді жүргізу;
- электрондық пошта хабарламаларын өңдеу ережелері қолданылғанға дейін көрсетілген тақырыптарды орталықтандырылған түрде алып тастау мүмкіндігін қамтамасыз ету;
- электрондық пошта хабарламаларын олардың параметрлеріне негізделген өңдеу ережелерін іздеу және сүзу мүмкіндігін қамтамасыз ету, сондай-ақ ережелерде пайдаланылған жіберушілер мен алушылардың тізімдеріне түсініктемелер қосу;
- орталықтандырылған басқарумен кластер конфигурациясында орналастыруды қолдау (көлденең және тік масштабтау үшін);
- ережелерді клондау және оларды тізімге сүйреп апару арқылы басымдықты өзгерту мүмкіндігі;
- Ережелерді орнатқан кезде, хабарламаға тек іске қосылатын ереженің нәтижесіне ғана емес, сонымен қатар әрбір қауіпсіздік модулінің бөлек іске қосылу нәтижесіне де негізделіп ескертпелер қосу мүмкіндігі болуы керек;
- веб-интерфейс арқылы конфигурациясы бар SIEM жүйесіне оқиғаларды жариялау мүмкіндігі;
- белгілі бір уақыт аралығында зиянды, фишингтік және спам мазмұны бар хабарламаларды қоса алғанда, қауіпті электрондық пошта хабарламаларын жиі алған пайдаланушылар туралы статистикалық ақпаратты жасауды және көрсетуді қамтамасыз ету;
- электрондық пошта хабарламасының мәтініндегі құпия сөздерді автоматты түрде анықтау және оларды қосымшаларда қамтылған құпия сөзбен қорғалған Microsoft Office құжаттарын тексеру үшін пайдалану мүмкіндігін қамтамасыз ету.

Microsoft Exchange серверлеріне арналған антивирустық және спам сүзгілеу бағдарламалық жасақтамасына қойылатын талаптар

Microsoft Exchange серверлеріне арналған антивирустық және спам сүзгілеу бағдарламалық жасақтамасы келесі операциялық жүйелерді іске қосатын компьютерлерде жұмыс істеуі керек:

1. Microsoft Windows Server 2022 Standard немесе Datacenter;
2. Microsoft Windows Server 2019 Standard немесе Datacenter;
3. Microsoft Windows Server 2016 Standard немесе Datacenter.

Microsoft Exchange серверлеріне арналған антивирустық және спам сүзгілеу бағдарламалық жасақтамасы Microsoft Exchange Server бағдарламалық жасақтамасының келесі нұсқаларында жұмыс істеуі керек:

1. Microsoft Алмасу 2019 сервері келесі рөлдердің кем дегенде біреуінде орналастырылған: пошта жәшігі немесе шеткі тасымалдау.
2. Microsoft Алмасу 2016 сервері келесі рөлдердің кем дегенде біреуінде орналастырылған: пошта жәшігі немесе шеткі тасымалдау.
3. Microsoft Алмасу Server 2013 SP 1 келесі рөлдердің кем дегенде біреуінде орналастырылған: пошта жәшігі, шеткі тасымалдау немесе клиентке кіру сервері (CA S).

консолін пайдаланып іске асырылуы және келесі операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі керек:

1. Microsoft Windows Server 2022 Standard немесе Datacenter;
2. Microsoft Windows Server 2019 Standard немесе Datacenter;
3. Microsoft Windows Server 2016 Standard немесе Datacenter;
4. Microsoft Windows Server операциялық жүйелері негізгі режимде.
5. Microsoft Windows 11 (x64);
6. Microsoft Windows 10 (x64).

Кез келген бағдарлама компонентін (Қауіпсіздік сервері немесе Басқару консолі) орнату үшін Microsoft Windows KB2999226 жаңарту бумасы қажет.

Microsoft Exchange серверлеріне арналған антивирустық қорғау және спамды сүзу бағдарламалық жасақтамасы келесі функцияларды қамтамасыз етуі керек:

- Microsoft Exchange бағдарламасында DAG-пен үйлесімділік;
- Кіріс және шығыс электрондық пошта хабарламалары ағынындағы, соның ішінде қосымшалардағы барлық вирус түрлерін, құрттарды, трояндарды және басқа да зиянды бағдарламаларды сұраныс бойынша іздеу және жою;

- Microsoft Exchange серверінде сақталған хабарламалардағы (қоғамдық қалталарды қоса алғанда), соның ішінде қосымшалардағы барлық вирус түрлерін, құрттарды, трояндарды және басқа да зиянды бағдарламаларды нақты уақыт режимінде іздеу және жою;
- эвристикалық анықтау әдістерінің болуы;
- сервер жүктемесін айтарлықтай арттырмай, барлық нысандардың антивирустық дерекқорлардың ең соңғы нұсқасын пайдаланып өңделетініне көз жеткізу үшін сервердегі пошта қоймасын және жалпы қалталарды фондық сканерлеу;
- жұқтырған мұрағаттарды емдеу мүмкіндігі;
- зиянды ғана емес, сонымен қатар ықтимал қауіпті қосымшаларды, мысалы: жарнамалық бағдарламаларды, деректерді жинау бағдарламаларын, ақылы сайттарға арналған автоматты тергіштерді және шабуылдаушылар өз мақсаттары үшін пайдалана алатын басқа да утилиталарды анықтау және жою мүмкіндігі;
- электрондық поштаның негізгі мәтініндегі зиянды және фишингтік сілтемелерді анықтау мүмкіндігі;
- өзгертілген хабарламалардың көшірмелерін резервтік сақтау орнында сақтау, бұл нысанды дұрыс емес өңдеу жағдайында маңызды ақпаратты қалпына келтіруге мүмкіндік береді;
- резервтік сақтау орнында нысанды оңай табуға арналған іздеу параметрлерінің жиынтығы;
- бедел бұлттық қызметтерін пайдалана отырып, қосымша тексеру деңгейі;
- ұйымнан тыс деректерді жібермей тексеруге мүмкіндік беретін жеке бедел қызметімен интеграциялау мүмкіндігі;
- қауіптерді блоктау үшін күрделі файлдарды ауытқуларға ашу және талдауға мүмкіндік беретін қауіпсіздік компонентінің болуы;
- хабарламалардағы және электрондық пошта тақырыптарындағы мәтіндерді тыйым салынған сөздерге тексеру мүмкіндігі.
- хаттың әртүрлі параметрлерін, мысалы, жіберуші мен алушының мекенжайларын, хат өлшемін және хабарлама тақырыбының өрістерін тексеру;
- спуфингтен қорғау (электрондық пошта хабарламасының шынайы авторын жасыру үшін жіберушінің мекенжайын жалған жасау).
- өзіңіздің «қара» және «ақ» тізімдеріңізге негізделген жіберушінің мекенжайы (электрондық пошта және/немесе IP мекенжайы) бойынша хабарламаларды сүзу немесе сүзгіден шығару;
- Sender Policy Framework (SPF) технологиясын пайдаланып домен үшін рұқсат етілген мекенжайлар тізімімен салыстыру ;
- мазмұнды сүзуді пайдалану (электрондық поштаның мазмұнын, соның ішінде Тақырып тақырыбын және тіркеме файлдарын талдау);
- қауіпсіздік параметрлеріне кіруді шектеу үшін пайдаланушы/әкімші рөлдерін пайдалану мүмкіндігі;
- Windows оқиғалар журналындағы оқиғаларға негізделген бағдарлама параметрлеріндегі өзгерістерді аудиттеу;
- бағдарламаның күйін бақылау, бағдарламаның жұмыс статистикасын алу және Windows PowerShell ортасындағы командаларды пайдаланып, спамға қарсы мекенжайлардың ақ және қара тізімдерін басқару ;

- мазмұнды сүзуді пайдалану (электрондық поштаның мазмұнын, соның ішінде Тақырып тақырыбы мен файл атауларын талдау);
- макростары бар Microsoft Office файлдарын сүзу мүмкіндігі;
- спам немесе фишинг және зиянды сілтемелер бар хабарламаларды тексеру және жою мүмкіндігі;
- сурет қосымшаларын белгілі спам хабарлама қолтаңбаларымен сәйкестікке тексеру;
- қауіпсіздік жүйесінің жұмысы туралы есептерді жасау;
- есептерді әкімшілерге кесте бойынша автоматты түрде жіберу мүмкіндігі;
- антивирустық дерекқорларды өндірушінің веб-сайттарынан да, ұйымның ішкі желілік ресурстарынан да жаңарту мүмкіндігі;
- Exchange Web Services көмегімен пошта жәшіктері мен жалпы қалталарды фондық сканерлеу мүмкіндігі;
- HTML форматындағы егжей-тегжейлі есептер;
- көрсетілген электрондық пошта мекенжайларына есептер мен хабарландырулар жіберу мүмкіндігі;
- бағдарламаның жұмысын System Center - Operations Manager көмегімен бақылау;
- Active Directory-мен интеграция;
- қорғау мәртебесін орталықтандырылған түрде қарау;
- жүйелік әкімші рөлдерін тарату мүмкіндігі.

Windows ОЖ негізіндегі бағдарламалық жасақтаманы орталықтандырылған басқаруға, бақылауға және жаңартуға қойылатын талаптар

Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық жасақтамасы келесі операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі керек:

1. Windows Server 2012 R2 Standard/Деректер орталығы/Ең маңызды ақпарат/Қор /Сервердің негізгі 64-биттік нұсқасы.
2. Windows Server 2016 Standard/Деректер орталығы/Ессенциалдар/Сервер ядросы (параметрлері орнатулар) (LTSB) 64-бит.
3. Windows Server 2019 Standard/Деректер орталығы/Core 64-бит.
4. Windows Server 2022 Standard/Деректер орталығы/Core 64-бит.
5. Windows Server 2025 Standard/Деректер орталығы/Core 64-бит.
6. Windows сақтау сервері 2019 64-бит.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек:

1. VMware vSphere 6.7.
2. VMware vSphere 7.0.
3. Microsoft Hyper-V Server 2019 64- биттік .
4. Microsoft Hyper-V Server 2022 64- биттік .
5. Citrix XenServer 7.1 LTSR.
6. Citrix XenServer 8.x.
7. Parallels Desktop 18.
8. Oracle VM VirtualBox 7.x.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық жасақтамасы келесі ДҚБЖ нұсқаларымен жұмыс істеуі керек:

1. Microsoft SQL Server 2016 (барлық басылымдар) 64-бит.
2. Microsoft SQL Windows / Linux 64-биттік жүйесіне арналған Server 2017 (барлық басылымдар) .
3. Microsoft SQL Windows / Linux 64-биттік жүйесіне арналған Server 2019 (барлық басылымдар) (қосымша қадамдар қажет).
4. Microsoft SQL Windows / Linux 64-биттік жүйесіне арналған Server 2022 (барлық басылымдар) .
5. MySQL 5.7 қауымдастығының 32-биттік/64-биттік нұсқасы.
6. MySQL 8.0 қауымдастығының 32-биттік/64-биттік нұсқасы.
7. MariaDB 10.5 (10.5.17 және одан кейінгі нұсқасы) 32 биттік/64 биттік.
8. MariaDB Галера InnoDB сақтау жүйесі бар 10.3 32-биттік/64-биттік кластер .
9. PostgreSQL 13.x 64-бит.
10. PostgreSQL 14.x 64-бит.
11. PostgreSQL 15.x 64-бит.
12. Postgres Pro 13.x Windows/Linux 64-бит.
13. PostgreSQL 14.x Windows/Linux 64-бит.

Вирусқа қарсы бағдарламалық жасақтама келесі функцияларды орындауы керек:

- қорғалатын түйіндер санына байланысты орталықтандырылған басқару, мониторинг және жаңарту құралын орнатуға арналған архитектураны таңдау;
- ұйымдағы компьютерлік және пайдаланушы тіркелгілері туралы деректер алу үшін Active Directory-ден ақпаратты оқу;
- IP мекенжайы, ОС түрі және AD OU орналасқан жері бойынша тасымалдау параметрлері ;
- Желіде жаңа компьютерлер пайда болған кезде компьютерлік тіркелгілерді басқару топтары арасында автоматты түрде тарату; AD OU-дағы IP мекенжайы, ОС түрі және орналасуы бойынша тасымалдау ережелерін конфигурациялау мүмкіндігі;
- антивирустық қорғау бағдарламалық жасақтамасын орталықтандырылған орнату, жаңарту және жою;
- орталықтандырылған конфигурация, басқару;
- қауіпсіздік құралдарының жұмысы туралы есептерді және статистикалық ақпаратты қарау;
- басқару орталығын пайдаланып үйлесімсіз қолданбаларды орталықтандырылған түрде жою (қолмен және автоматты);
- саясат пен тапсырмаларға енгізілген өзгерістер тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;
- антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін - RPC, GPO, басқару жүйесін пайдалану; жергілікті орнату үшін - дербес орнату пакетін жасау мүмкіндігі;
- пайдаланушы кірген тіркелгіге, ағымдағы IPv4 мекенжайына, сондай-ақ компьютер орналасқан OU немесе қауіпсіздік тобына байланысты антивирустық шешім параметрлерін қайта анықтайтын қауіпсіздік саясатында арнайы триггерлерді көрсету;

- қайта бөлу жүретін триггерлер иерархиялары;
- жүктелген жаңартуларды клиенттік машиналарға таратпас бұрын орталықтандырылған басқару бағдарламалық жасақтамасын пайдаланып тексеру;
- жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс станцияларына жеткізу;
- желідегі виртуалды машиналарды тану және егер бұл машиналар бір физикалық серверде орналасқан болса, олардың арасында орындалатын тапсырмалардың жүктеме балансын бөлу;
- әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есеп беру нысандарын теңшеу мүмкіндігі бар көп деңгейлі басқару жүйесін құру;
- кез келген деңгейдегі әкімшілік серверлер иерархиясын құру және жоғарғы деңгейден бастап бүкіл иерархияны орталықтан басқару мүмкіндігі;
- басқару серверлері үшін көп пәтерлі қолдау ;
- байланыс арналары арқылы да, машиналық сақтау құралдары арқылы да әртүрлі көздерден бағдарламалық жасақтама мен вирусқа қарсы дерекқорларды жаңарту;
- басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлттық серверлеріне қол жеткізу;
- клиенттік компьютерлерге лицензияларды автоматты түрде тарату;
- пайдаланушылардың компьютерлерінде орнатылған бағдарламалық жасақтама мен аппараттық құралдардың тізімдемесі;
- орнатылған антивирустық қорғау қолданбаларының жұмысындағы оқиғалар туралы хабарландыру механизмінің болуы және олар туралы электрондық пошта арқылы хабарландыруларды жіберу конфигурациясы;
- iOS MDM сервері арқылы мобильді құрылғыны басқару функциясы ;
- көрсетілген оқиғалар туралы SMS хабарламалар жіберу;
- басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату;
- басқару жүйесіндегі желілік жүктемені азайту үшін ұйымдағы кез келген компьютерді жаңарту релелік орталығы ретінде белгілеу;
- басқару жүйесіндегі желілік жүктемені азайту үшін ұйымдағы кез келген компьютерді антивирустық агент оқиғаларын жіберу орталығы, таңдалған клиенттік компьютерлер тобы немесе орталықтандырылған басқару сервері ретінде белгілеу;
- антивирустық қорғау оқиғалары, инвентаризация деректері және орнатылған бағдарламаларға арналған лицензиялау деректері туралы графикалық есептерді жасау;
- алдын ала конфигурацияланған стандартты есептердің болуы ;
- есептерді PDF және XML файлдарына экспорттау;
- антивирустық бағдарламалық жасақтама орнатылған барлық желілік ресурстар үшін резервтік көшірмелерді сақтауды және карантинге алынған нысандарды орталықтандырылған басқару;
- басқару серверінде аутентификация үшін ішкі тіркелгілерді жасау;
- басқару жүйесінің кіріктірілген құралдарын пайдаланып, басқару жүйесінің резервтік көшірмесін жасау;
- Windows ақаулықтарды кластерлеуді қолдау ;
- қолдау интеграция Windows Certificate Authority қызметімен ;
- пайдаланушының өзіне-өзі қызмет көрсету порталының болуы;

- Өзіне-өзі қызмет көрсету порталы пайдаланушыларға мобильді құрылғыға басқару агентін орнату, мобильді құрылғыларды көру, бұғаттау командаларын жіберу, құрылғыны іздеу және пайдаланушының мобильді құрылғысындағы деректерді жою үшін қосылу мүмкіндігін қамтамасыз етуі тиіс;
- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- Microsoft Azure және Google Cloud бұлттық инфрақұрылымындағы орнатулар;
- OpenAPI интеграциясы ;
- WEB консолін пайдаланып антивирустық қорғауды басқару;
- басқару консолі арқылы Windows ОЖ орналастыруды басқару мүмкіндігі;
- орталықтандырылған басқару құралдары үшін алдын ала конфигурацияланған пайдаланушы рөлдерінің қолжетімділігі ;
- пайдаланушы тіркелгілеріне байланыстырылатын арнайы көрсетілген рұқсаттар жиынтығы бар мамандандырылған рөлдерді жасау мүмкіндігі іске асырылуы керек;
- басқару консолінен RDP немесе стандартты құралдар арқылы қосылу мүмкіндігі;
- Windows жұмыс үстеліне қосылымды ортақ пайдалану мүмкіндігі (Windows Жұмыс үстелі Бөлісу);
- пайдаланушыдан қашықтан қосылуға рұқсат беру сұралуы керек;
- ОС кескіндерімен жұмыс істеуге арналған құралдардың қолжетімділігі: Физикалық немесе виртуалды машина негізінде мақсатты ОС кескінін жасау, кескінді әкімші таңдаған компьютерлерге , соның ішінде металлға орнату металл);
- бұрын жасалған кескінге драйвер жиынтықтарын қосу мүмкін болуы керек;
- ОС орнатқаннан кейін сценарийлерді іске қосу немесе қосымша бағдарламалық жасақтаманы автоматты түрде орнату мүмкіндігі;
- операциялық жүйенің кескінін дистрибутивтерден (WIM) импорттау мүмкіндігі
- компьютерде орнатылған үшінші тарап бағдарламалық жасақтамасына арналған лицензияны басқару жүйесінің болуы, лицензияны пайдаланудың кез келген бұзылуы немесе лицензияның жарамдылық мерзімі туралы әкімшіге хабарлау мүмкіндігі;
- үшінші тарап қолданбалары (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) үшін орнату пакеттерін автоматты түрде жасау және осы қолданба пакеттерін компьютерлерге автоматты түрде орталықтандырылған орнату;
- деректерді шифрлауды басқару функциясын қолдау;
- syslog немесе CEF/LEEF форматында жіберу мүмкіндігі
- Әкімшілік консоліне рұқсатсыз кіру қаупін азайту үшін екі сатылы тексеру;
- пайдаланушы тіркелгісінің параметрлерін өзгерткеннен кейін қосымша аутентификацияны пайдалану.
- IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғыларды қамтитын желілерге сұраныс беру мүмкіндігі.
- Microsoft операциялық жүйесі бар пайдаланушылардың компьютерлері мен серверлеріндегі орнатылған қолданбалар мен операциялық жүйедегі осалдықтарды автоматты түрде іздеу және жабу Терезелер ;
- Әкімшілік серверді жоғары қолжетімділік жүйесі ретінде орналастыру мүмкіндігі;
- оқшауланған желідегі үшінші тарап бағдарламаларындағы (Microsoft бағдарламаларынан басқа) жаңартуларды орнату және осалдықтарды түзету мүмкіндігі;

- Windows және Linux негізіндегі клиенттік құрылғыларды қашықтан диагностикалау (іздерді, оқиғалар журналдарын, дамптарды алу, қолданбаларды тоқтату және іске қосу);
- Linux операциялық жүйесін іске қосатын басқарылатын құрылғылардағы тіркелгілер үшін жергілікті әкімші құқықтарын қайтарып алу мүмкіндігі;
- Linux операциялық жүйесін іске қосатын басқарылатын құрылғылардағы жергілікті тіркелгінің құпия сөзін өзгерту мүмкіндігі.

Linux ОЖ негізінде орталықтандырылған басқару, мониторинг және жаңарту үшін бағдарламалық жасақтамаға қойылатын талаптар

Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық жасақтамасы келесі операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі керек:

1. Debian GNU/Linux 12 (Bookworm) 64-бит.
2. Debian GNU/Linux 13 (Trixie) 64-бит.
3. Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64- бит .
4. Ubuntu сервері 24.04 LTS (Noble Numbat) 64 бит .
5. CentOS Stream 9 64-бит.
6. CentOS Stream 10 64-бит.
7. Red Hat Enterprise Linux Server 7.x 64- бит .
8. Red Hat Enterprise Linux Server 8.x 64- бит .
9. Red Hat Enterprise Linux Server 9.x 64- бит .
10. Red Hat Enterprise Linux Server 10.x 64- бит .
11. SUSE Linux Enterprise Server 12 (барлық қызмет пакеттері) 64-бит.
12. SUSE Linux Enterprise Server 15 (барлық қызмет пакеттері) 64-бит.
13. Astra Linux арнайы басылымы RUSB.10015-01 (соңғы жаңарту 1.6) 64-бит.
14. Astra Linux арнайы басылымы RUSB.10015-01 (соңғы жаңарту 1.7) 64-бит.
15. Astra Linux арнайы басылымы RUSB.10015-01 (соңғы жаңарту 1.8) 64-бит.
16. Astra Linux арнайы шығарылымы RUSB.10015-16 (1-нұсқа) (соңғы жаңарту 1.6) 64-бит.
17. Astra Linux арнайы басылымы RUSB.10015-17 (соңғы жаңарту 1.7.3) 64-бит.
18. Astra Linux арнайы басылымы RUSB.10015-03 (соңғы жаңарту 7.6) 64-бит.
19. Astra Linux арнайы басылымы RUSB.10015-37 (соңғы жаңарту 7.7) 64-бит.
20. Astra Linux Common Edition (соңғы жаңарту 2.12) 64-бит.
21. Alt SP Server 10 64-бит.
22. Alt SP жұмыс станциясы 10 64-бит.
23. Oracle Linux 7 64-биттік нұсқасы.
24. Oracle Linux 8 64-бит.
25. Oracle Linux 9 64-биттік нұсқасы.
26. V платформасы SberLinux OS сервері (SLO) 8.10.1 64 бит .
27. V платформасы SberLinux OS сервері (SLO) 9.5.1 64- бит .
28. V платформасы SberLinux OS сервері (SLO) 9.6 64 бит .
29. ҚЫЗЫЛ OS 7.3 серверінің 64-биттік нұсқасы.
30. ҚЫЗЫЛ OS 7.3 сертификатталған 64-биттік басылымы.

31. ҚЫЗЫЛ OS 8 64-бит.
32. ROSA "COBALT" 7.9 64-бит.
33. М ОС (Мәскеу электрондық мектебі) 12 серверінің 64- биттік нұсқасы .
34. Mostech серверінің 64-биттік нұсқасы.
35. MosOS 15.5 Arbat 64-бит.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек:

1. VMware vSphere 6.7.0.
2. VMware vSphere 7.0.3.
3. Microsoft Hyper-V Server 2019 64- биттік .
4. Microsoft Hyper-V Server 2022 64- биттік .
5. Citrix XenServer 7.x.
6. Citrix XenServer 8.2.
7. Parallels Desktop 18.
8. Oracle виртуалды машинасының VirtualBox 7.0.12 нұсқасы.
9. Ядроға негізделген виртуалды машина (барлығы қолдау көрсетілді Linux ОЖ).

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық жасақтамасы келесі ДҚБЖ нұсқаларымен жұмыс істеуі керек:

1. MySQL 5.7 қауымдастығының 32-биттік/64-биттік нұсқасы.
2. MySQL Standard Edition 8.0 (8.0.20 және одан кейінгі нұсқасы) 32-биттік/64-биттік.
3. MySQL Enterprise Edition 8.0 (8.0.20 және одан кейінгі нұсқасы) 32 биттік/64 биттік.
4. MySQL стандартты басылымы 8.4 32 биттік / 64 биттік .
5. MySQL Enterprise Edition 8.4 32 биттік / 64 биттік .
6. MariaDB 10.1 (10.1.30 және одан кейінгі нұсқасы) 32 биттік/64 биттік.
7. MariaDB 10.3 (10.3.22 және одан кейінгі нұсқасы) 32 биттік/64 биттік.
8. MariaDB 10.4 (10.4.20 және одан кейінгі нұсқасы) 32 биттік/64 биттік.
9. MariaDB 10.5 (10.5.27 және одан кейінгі нұсқасы) 32 биттік/64 биттік.
10. MariaDB 10.6 (10.6.20 және одан кейінгі нұсқасы) 32 биттік/64 биттік.
11. MariaDB 10.11 (10.11.10 және одан кейінгі нұсқасы) 32 биттік/64 биттік.
12. MariaDB InnoDB сақтау қозғалтқышы бар Galera Cluster 10.3 32-биттік/64-биттік .
13. PostgreSQL 13.x 64-бит.
14. PostgreSQL 14.x 64-бит.
15. PostgreSQL 15.x 64-бит.
16. PostgreSQL 15.x 64-бит (Corosync / Pacemaker кластері).
17. PostgreSQL 16.x 64-бит.
18. PostgreSQL 17 64-бит.
19. PostgreSQL 18 64-бит.
20. Postgres Pro 13.x (барлық басылымдар) 64-бит.
21. Postgres Pro 14.x (барлық басылымдар) 64-бит.
22. Postgres Pro 15.x (барлық басылымдар) 64-бит.
23. Postgres Pro 15. x 64- бит (кластер Коросинк / кардиостимулятор).
24. Postgres Pro 16.x (барлық басылымдар) 64-бит.

25. Postgres Pro 16. x Enterprise 64- bit (кіріктірілген жоғары қолжетімділік кластері).
26. Postgres Pro 17 (барлық басылымдар) 64-бит.
27. Postgres Pro 17 Enterprise 64- бит (кіріктірілген жоғары қолжетімділік кластері).
28. Postgres Pro 18 (барлық басылымдар) 64-бит.
29. Postgres Pro 18 Enterprise 64- бит (кіріктірілген жоғары қолжетімділік кластері).
30. V платформасы Pangolin 6.5.1 64-бит.
31. V Pangolin 6.5.1 64- биттік платформасы (кіріктірілген жоғары қолжетімділік кластері).
32. Jatoba 4 64-бит.
33. Jatoba 5 64-бит.
34. Tantor SE 1C 64-бит.

Вирусқа қарсы бағдарламалық жасақтама келесі функцияларды орындауы керек:

- антивирустық қорғау бағдарламалық жасақтамасын орталықтандырылған орнату, жаңарту және жою;
- орталықтандырылған конфигурация, басқару;
- қауіпсіздік құралдарының жұмысы туралы есептерді және статистикалық ақпаратты қарау;
- саясат пен тапсырмаларға енгізілген өзгерістер тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;
- қайта бөлу жүретін триггерлер иерархиялары;
- жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс станцияларына жеткізу;
- желідегі виртуалды машиналарды тану және егер бұл машиналар бір физикалық серверде орналасқан болса, олардың арасында орындалатын тапсырмалардың жүктеме балансын бөлу;
- әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есеп беру нысандарын теңшеу мүмкіндігі бар көп деңгейлі басқару жүйесін құру;
- кез келген деңгейдегі әкімшілік серверлер иерархиясын құру және жоғарғы деңгейден бастап бүкіл иерархияны орталықтан басқару мүмкіндігі;
- басқару серверлері үшін көп пәтерлі қолдау ;
- байланыс арналары арқылы да, машиналық сақтау құралдары арқылы да әртүрлі көздерден бағдарламалық жасақтама мен вирусқа қарсы дерекқорларды жаңарту;
- басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлттық серверлеріне қол жеткізу;
- клиенттік компьютерлерге лицензияларды автоматты түрде тарату;
- орнатылған антивирустық қорғау қолданбаларының жұмысындағы оқиғалар туралы хабарландыру механизмінің болуы және олар туралы электрондық пошта арқылы хабарландыруларды жіберу конфигурациясы;
- орнатылған бағдарламаларға арналған антивирустық қорғау оқиғалары және лицензиялау деректері туралы графикалық есептерді жасау;
- алдын ала конфигурацияланған стандартты есептердің болуы ;
- есептерді PDF және XML файлдарына экспорттау;

- антивирустық бағдарламалық жасақтама орнатылған барлық желілік ресурстар үшін резервтік көшірмелерді сақтауды және карантинге алынған нысандарды орталықтандырылған басқару;
- басқару серверінде аутентификация үшін ішкі тіркелгілерді жасау;
- Әкімшілік консоліне рұқсатсыз кіру қаупін азайту үшін екі сатылы тексеру;
- басқару жүйесінің кіріктірілген құралдарын пайдаланып, басқару жүйесінің резервтік көшірмесін жасау;
- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- WEB консолін пайдаланып антивирустық қорғауды басқару;
- әкімшілік серверге түсетін жүктемені азайту және корпоративтік желідегі деректер трафигін оңтайландыру үшін әкімшілік сервер арқылы да, тарату нүктелері арқылы да басқарылатын құрылғылардағы антивирустық дерекқорлар мен бағдарламалық модульдерді жаңарту және тарату;
- Басқарылатын құрылғыларға жүктелген жаңартуларды орнатпас бұрын, олардың функционалдығы мен қателерін тексеру үшін жаңартуды тексеру тапсырмасын пайдаланыңыз;
- антивирустық дерекқорлар мен бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары мүмкіндігін пайдаланыңыз;
- орталықтандырылған басқару серверлері арасында шифрлау кілттерін беру мүмкіндігі;
- басты сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйелерінде жұмыс істейтін серверлерді құл ретінде басқару;
- іс-шара үлгілерін экспорттау және импорттау мүмкіндігі;
- оқиғаларды SIEM жүйесіне CEF немесе LEEF форматтарында экспорттау мүмкіндігі;
- Android және iOS жүйелерінде мобильді құрылғыларды басқару мүмкіндігі ;
- басқарылатын құрылғыларға орнатылған бағдарламалар туралы ақпарат алу;
- Microsoft операциялық жүйесі бар пайдаланушылардың компьютерлері мен серверлеріндегі орнатылған қолданбалар мен операциялық жүйедегі осалдықтарды автоматты түрде іздеу және жабу Терезелер ;
- Samba домен контроллерлері бойынша құрылғыларды іздеу мүмкіндігі ;
- Windows ОЖ жұмыс істейтін әкімшілік серверден Linux ОЖ жұмыс істейтін әкімшілік серверге деректерді автоматты түрде беру мүмкіндігі;
- басқарылатын құрылғыларды қашықтан диагностикалау мүмкіндігі;
- кластерлік технологияны қолдау;
- басқарылатын құрылғылардан үйлесімсіз бағдарламалық жасақтаманы орталықтан жою мүмкіндігі;
- басқарылатын құрылғыларды орталықтан қайта жүктеу мүмкіндігі;
- құрылғының орналасқан жеріне байланысты бірдей немесе әртүрлі орталықтандырылған басқару серверлеріне қосылу үшін Linux құрылғылары бар жеке пайдаланушыларға қосылу профильдерін орнату мүмкіндігі;
- FreeIPA және ALD Pro домен контроллерлерін қолдау;
- Kerberos көмегімен домен аутентификациясын қолдау (сертификатқа негізделгенді қоса алғанда, бірыңғай кіру технологиясы).

Вирусқа қарсы дерекқорларды жаңартуға қойылатын талаптар

Жаңартылған антивирустық дерекқорлар келесі функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі керек:

- вирусқа қарсы дерекқорларды күнтізбелік күнде кемінде 24 рет жаңарту ережелерін жасау;
- байланыс арналары арқылы және оқшауланатын электрондық ақпарат тасымалдағыштарында қоса алғанда, бірнеше жаңарту жолдары;
- электрондық цифрлық қолтаңбаларды пайдалана отырып, жаңартулардың тұтастығы мен түпнұсқалығын тексеру.

Пайдалану құжаттамасына қойылатын талаптар

- Вирусқа қарсы бағдарламалық жасақтамамен бірге берілетін құжаттамада тиісті вирусқа қарсы бағдарламалық жасақтаманы орнату, конфигурациялау және пайдалану процесі егжей-тегжейлі сипатталуы керек.

Техникалық қолдау талаптары

Вирусқа қарсы бағдарламалық жасақтамаға техникалық қолдау көрсету келесідей болуы керек:

- Вирусқа қарсы қорғаныс өндірушісінің сертификатталған мамандары және оның Қазақстан Республикасы бойынша серіктестері электрондық пошта және интернет арқылы орыс және қазақ тілдерінде ұсынады.
- Вирусқа қарсы шешім өндірушісінің веб-сайтында вирусқа қарсы шешімге техникалық қолдау көрсетуге арналған арнайы бөлім, жаңартылған білім базасы және бағдарламалық жасақтаманы пайдаланушыларға арналған форум болуы керек.

Техникалық сипаттамалар бойынша мына мекенжайға хабарласыңыз: Рязанов Д.В., тел. +7-727-244-52-73, электрондық пошта : dim@kazrosgas.kz

Қол қойған	Рязанов Дмитрий Владимирович
Қол қойылған күні	09.11.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1268301
способом Запрос ценовых предложений на понижение

Лот № (76 Т, 4575372) Лицензия

Заказчик: Товарищество с ограниченной ответственностью "КазРосГаз"
Организатор: Товарищество с ограниченной ответственностью "КазРосГаз"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	76 Т
Наименование и краткая характеристика	Лицензия, на программный продукт (кроме услуг по предоставлению лицензии)
Наименование категории ОКТРУ	Лицензия
Дополнительная характеристика	Тип: годовая лицензия на антивирусную программу
Количество	1.000
Единица измерения	Штука
Место поставки	КАЗАХСТАН, г.Алматы, ул.Байзакова, 280
Условия поставки	DDP
Срок поставки	С даты подписания договора по (включительно) 12.2026
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

Предоставление лицензии на право использования антивирусного программного обеспечения защиты рабочих станций, серверов и мобильных устройств на 70 пользователей.

Срок действия предоставляемой лицензии должен быть не менее одного календарного года с момента предоставления лицензии.

В наличии действующая лицензия на право использования программного обеспечения Kasp ersky Total Security for Business на 70 пользователей.

Антивирусные средства должны включать:

- программные средства антивирусной защиты для рабочих станций Windows;
- программные средства антивирусной защиты для файловых серверов Windows;
- программные средства антивирусной защиты для рабочих станций MacOS;
- программные средства антивирусной защиты для рабочих станций и серверов Linux;
- программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);
- программные средства антивирусной защиты веб-трафика;

- программные средства антивирусной защиты и фильтрации спама с помощью отдельного сервера
- программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux;
- программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange;
- программные средства централизованного управления, мониторинга и обновления;
- обновляемые базы данных сигнатур вредоносных программ и атак;
- эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

Требования к программным средствам антивирусной защиты для рабочих станций

Windows

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:

1. Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;
2. Windows 8 Professional / Enterprise (32 / 64-разрядная);
3. Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
4. Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise/Enterprise multi-session;
5. Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise;
6. Windows 11 Pro / Pro для рабочих станций / Education / Enterprise.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

- формировать область защиты для функции защиты папок общего доступа от внешнего шифрования;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
- фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
- распознавания и блокировку фишинговых и небезопасных сайтов;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
- защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
- контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
- создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;

- контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
- управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей /групп), в рамках контроля устройств;
- записи в журнал событий о записи и/или удалении файлов на съемных дисках;
- назначение приоритета для правил доступа к устройствам с файловой системой;
- контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
- защиты от атак типа BadUSB;
- защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
- управления параметрами через доверенные программы удаленного администрирования;
- установки только выбранных компонентов программного средства антивирусной защиты;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- запуска задач по расписанию и/или сразу после запуска приложения;
- гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- проверки целостности антивирусной программы;
- добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
- импорта и экспорта списков правил и исключений в XML-формат;
- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
- наличие защищенного хранилища для отчетов о работе антивируса;
- включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
- интеграции с Windows Defender Security Center;
- наличие поддержки Antimalware Scan Interface (AMSI);
- наличие поддержки Windows Subsystem for Linux (WSL);
- защитить паролем восстановление объектов из резервного хранилища;

- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
- наличие инструмента мониторинга сети по протоколам TCP и UDP;
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- установки ограничение длительности выполнения задачи;
- ставить задачи проверки в очередь, если проверка уже выполняется;
- обновление без перезагрузки системы;
- настроить доступ пользователей к мобильным устройствам в приложении Android Debug Bridge (ADB);
- заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;
- настроить права печати для пользователей;
- наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;
- наличие совместимости с Azure WVD;
- настроить доступ пользователей к мобильным устройствам в приложении iTunes;
- запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
- восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;
- поддержка двухфакторной аутентификации при полнодисковом шифровании;
- шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);
- наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;
- шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
- возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
- поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании;
- возможность настроить исключения и ограничить доступ ко всем Bluetooth-устройствам кроме устройств ввода;
- возможность обновления приложения без перезагрузки операционной системы;
- возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО;
- возможность запретить внешнее управление службами приложения;
- возможность выбирать предустановленные исключения из проверки и доверенные приложения;

- возможность задать разрешение отдельному пользователю на экспорт настроек в конфигурационный файл;
- возможность мониторинга и отзыва временных паролей на доступ к приложению, позволяющий сохранять историю паролей (до 30 дней) и контролировать статус (Активен, Истек, Отозван);
- возможность разрывать подключение к веб-ресурсам, запрещенными правилами Веб-Контроля, сразу после применения политики;
- возможность настраивать разные наборы компонентов для разных типов операционных систем в инсталляционном пакете;
- возможность выбирать предустановленные исключения из проверки и доверенные приложения;
- возможность блокировать сетевые соединения по устаревшему протоколу TLS 1.0;
- поддержка протокола Kerberos для аутентификации приложения через прокси-сервер для доступа в интернет;
- возможность указывать хеш файла для исключения приложения из проверки.

Требования к программным средствам антивирусной защиты для серверов Windows

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий:

1. Windows Small Business Server 2011 Essentials / Standard (64-разрядная), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2;
2. Windows MultiPoint Server 2011 (64-разрядная);
3. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
4. Windows Web Server 2008 R2 Service Pack 1 и выше;
5. Windows Server 2012 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
6. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
7. Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);
8. Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);
9. Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core).
10. Windows Server 2025 Standard / Datacenter.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;

- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
- защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
- установки только выбранных компонентов программного средства антивирусной защиты;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- проверки целостности антивирусной программы;
- добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
- наличие защищенного хранилища для отчетов о работе антивируса;

- включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
- интеграции с Windows Defender Security Center;
- наличие поддержки Antimalware Scan Interface (AMSI);
- наличие поддержки Windows Subsystem for Linux (WSL);
- защитить паролем восстановление объектов из резервного хранилища.
- импорта и экспорта списков правил и исключений в XML-формат;
- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
- создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
- формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
- запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
- поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- возможность установки ограничения длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется;
- обновление без перезагрузки системы;
- настройки прав доступа (чтение / запись) для портативных устройств (MTP), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам;
- заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;
- настроить права печати для пользователей;
- наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;
- наличие совместимости с Azure WVD;
- возможность обновления приложения без перезагрузки операционной системы;
- возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО.
- возможность запретить внешнее управление службами приложения.
- возможность использования предустановленных исключений из проверки и доверенных приложений, предназначенных для быстрой настройки доверенной зоны

для работы приложения на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager;
- поддержка протокола Kerberos для аутентификации приложения через прокси-сервер для доступа в интернет;
- возможность указывать хеш файла для исключения приложения из проверки.

Требования к программным средствам антивирусной защиты для рабочих станций Mac

Программные средства антивирусной защиты для рабочих станций Mac должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

1. macOS 12 - 15;

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- резидентный антивирусный мониторинг;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- автоматическое обновление антивирусных баз по расписанию;
- резервное копирование зараженных файлов перед их удалением, для возможности восстановления;
- эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
- защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
- блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
- проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);
- контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем
- ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- задавать исключения при проверке указанных областей на уровне перехватов файловых операций;
- автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены;

- ограничивать загрузку процессора приложением при выполнении задач поиска вредоносного ПО;
- включения облачного режима и использования облегченной версии баз вредоносного ПО, для снижения нагрузки на ресурсы операционной системы;
- пропускать сканирование системного тома, доступного только для чтения, во время выполнения задач проверки по требованию;
- анализа активности приложений в операционной системе с использованием шаблонов опасного поведения (BSS);
- установки из файла .pkg через JAMF;
- автоматического сканирования внешних дисков при их подключении;
- поддержки клиентских сертификатов;
- проверки вложений входящих и исходящих сообщений электронной почты на наличие в них вредоносного ПО и других угроз;
- управления доступом пользователей к установленным или подключенным к компьютеру устройствам;
- блокировки несанкционированных подключений к компьютеру во время работы в интернет или локальной сети и контроль сетевой активности приложений;
- откат действий вредоносного программного обеспечения, связанных с его файловой, системной или сетевой активностью в ОС;
- защита от эксплойтов;
- централизованного управления всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 32-битных операционных систем следующих версий:

1. Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:

1. AlmaLinux OS 8.6, 8.7, 8.8, 8.9.
2. AlmaLinux OS 9.4, 9.5, 9.6.
3. AlterOS® 2025.
4. Amazon™ Linux 2023.
5. Astra Linux Common Edition 2.12.
6. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
7. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
8. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
9. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).
10. Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6).

11. Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
12. Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3).
13. Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).
14. CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
15. CentOS Stream 8.
16. CentOS Stream 9.
17. CentOS Stream 10.
18. Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
19. Debian GNU/Linux 13.0, 13.1, 13.2.
20. EMIAS 1.0.
21. EulerOS 2.0 SP10.
22. Fedora 41.
23. Kylin 10.
24. Linux Mint 21.3.
25. Linux Mint 22.2.
26. Mostech 12 release 2021.1.
27. openSUSE Leap 15.6.
28. Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
29. Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9.
30. Oracle Linux 9.4, 9.5, 9.6.
31. Red Hat® Enterprise Linux® 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
32. Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9.
33. Red Hat Enterprise Linux 9.4, 9.5, 9.6.
34. Red Hat Enterprise Linux 10.0, 10.1.
35. Rocky Linux 8.6, 8.7, 8.8, 8.9.
36. Rocky Linux 9.4, 9.5, 9.6.
37. SberLinux 8.10, 9.1, 9.5, 9.6.
38. SberOS 3.4.0, 3.5.0.
39. SUSE Linux Enterprise Server 12.5, 12.6, 12.7.
40. SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7.
41. Ubuntu® 22.04 LTS.
42. Ubuntu 24.04 LTS.
43. Альт Образование 10.
44. Альт Образование 11.
45. Альт Рабочая Станция 11.
46. Альт Сервер 11.
47. Альт СП Сервер релиз 10.
48. Альт СП Рабочая Станция релиз 10.
49. Атлант, сборка Alcyone, версия 2022.02.
50. Гослинукс 7.2.
51. МОС 12 Сервер release 2021.1.
52. МосОС 15.5 Arbat.
53. МСВСФЕРА 9.4 АРМ.
54. МСВСФЕРА 9.4 СЕРВЕР.

55. ОС МЭШ 12 Для всех пользователей (без телеметрии и без поддержки ДИТ) release 20 21.1.
56. ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ) release 2021.1.
57. ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ) release 2021.1.
58. ОСнова 2.14.
59. ОСнова 3.0.5.
60. РЕД ОС® 7.3.
61. РЕД ОС 8.0.
62. РОСА "Кобальт" 7.9 Рабочая станция.
63. РОСА "Кобальт" 7.9 Сервер.
64. РОСА "Хром" 12 Рабочая станция.
65. РОСА "Хром" 12 Сервер.
66. СинтезМ-Клиент 8.6.
67. СинтезМ-Сервер 8.6.

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

1. Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
2. CentOS Stream 9.
3. EulerOS 2.0 SP10.
4. SUSE Linux Enterprise Server 15.
5. Ubuntu 22.04 LTS.
6. Альт СП Рабочая Станция релиз 10.
7. Альт СП Сервер релиз 10.
8. РЕД ОС 8.0.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- резидентного антивирусного мониторинга;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- проверку ресурсов доступных по SMB / NFS;
- возможность проверки памяти ядра;
- эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
- проверку входящих и исходящих сообщений электронной почты;

- наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
- защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
- включения опции блокирования файлов во время проверки;
- помещение подозрительных и поврежденных объектов на карантин;
- перехвата и проверки файловых операций на уровне SAMBA;
- управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- экспортировать и сохранять отчеты в форматах HTML и CSV;
- гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
- управления через пользовательский графический интерфейс без root прав;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
- управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
- проверки съемных дисков;
- отслеживания во входящем сетевом трафике активности, характерной для сетевых атак;
- проверки трафика, поступающего на компьютер пользователя по протоколам HTTP /HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым
- получения данных о действиях программ на компьютере пользователя;
- получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
- создание файлов трассировки при запуске программы;
- получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
- проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;
- сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий;
- исключения процессов из проверки памяти процессов в общих параметрах программы;
- оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles;
- исключения трафика из проверки программой;
- использовать формат JSON для запросов и вывода информации, а также для экспорта и импорта параметров программы и параметров задач;

- установки и работы на устройствах с операционными системами для архитектуры Arm;
- работать в режиме информирования пользователя в случае обнаружения угроз или при обнаружении попытки доступа к устройству;
- возможность управлять запуском приложений на защищаемых устройствах с помощью правил контроля в режимах списка запрещенных или разрешенных приложений;
- автоматический перезапуск приложения при обновлении;
- возможность задать ограничение на использование ресурсов процессора;
- возможность в автоматическом режиме выключить компоненты защиты и задачи проверки при запуске приложения после установки;
- уведомления пользователя о работе компонентов и задач в графическом пользовательском интерфейсе;
- возможность читать память процессов, не останавливая их (ядра Linux начиная с версии 3.4);
- возможность управлять доступом пользователей к веб-ресурсам;
- возможность управлять запуском приложений на защищаемых устройствах;
- функция мониторинга стабильности собственной работы приложения;
- защита от эксплойтов с возможностью настройки исключения объектов из проверки;
- возможность настроить список пользователей или групп пользователей контроля устройств, для которых добавленные устройства будут доверенными;
- возможность разрешать доступ к устройствам хранения данных только на чтение;
- возможность настраивать исключения для отдельных компонентов приложения при использовании прокси-сервера;
- возможность настраивать исключения из перехвата трафика;
- возможность временного исключения из проверки файлов журналов баз данных;
- возможность экспорта и импорта списков исключений в политиках и задачах, применяемых к приложению;
- возможность настраивать отмену запуска запланированных задач на устройстве, работающем от аккумулятора;
- возможность вывода списка функций приложения в командной строке, информацию об их статусах (используется или не используется) и технологиях Linux, с помощью которых реализованы эти функции приложения;
- возможность защиты от атак типа BadUSB;
- возможность отображать в командной строке и в графическом интерфейсе информацию о действующей на устройстве политике и профилях политики.

Требования к программным средствам антивирусной защиты мобильных устройств

Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:

1. Android 5.0 и выше (включая Android 12L, исключая Go Edition);
2. iOS 15 и выше или iPadOS 15 и выше;

В программном средстве антивирусной защиты смартфонов для ОС Android должны быть реализованы следующие функциональные возможности:

- постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
- проверка файловой системы устройства по требованию и по расписанию;
- мгновенная проверка устанавливаемых приложений
- блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
- наличие хранилища для изолирования зараженных объектов;
- обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
- блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
- поддержка белых списков разрешенных приложений;
- блокировка системных приложений, в рамках контроля запуска приложений;
- отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);
- заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
- указать параметры подключения к wi-fi сетям;
- указать обязательные к установке приложения;
- блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
- создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
- поддержка технологий Samsung KNOX1 и KNOX2;
- указать разрешенные версии приложений при создании правил Контроля приложений для Androidустройств.

В программном средстве защиты смартфонов для ОС Apple iOS должны быть реализованы следующие функциональные возможности:

- удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
- отправки команды блокирования и удаления данных;
- создавать групповые политики безопасности мобильных устройств;
- удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;
- получать отчеты и статистику о работе мобильных устройств пользователей;

- блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;
- централизованного управления с помощью единой консоли управления;
- наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.
- запретить изменение настроек Bluetooth для iOS MDMустройств.

Требования к системе защиты веб-трафика

Система должна поставляться в виде

- ISO-образа, с предустановленной операционной системой, прокси-сервером и средствами защиты и контроля трафика
- RPM- или DEB- пакета, содержащего дистрибутив программы для защиты и контроля трафика

Система должна поддерживать установку и работу на следующих операционных системах:

- CentOS 7.7.
- Rocky Linux 8.10, 9.4.
- Red Hat Enterprise Linux версии 7.7, 8.10, 9.4.
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS.
- Debian 9.13, 10.13, 11.10, 12.10.
- SUSE Linux Enterprise Server 15 SP1.
- РЕД ОС 7.3, 8.0.
- Альт Сервер 10.

Система должна поддерживать установку на физический и виртуальный сервер, для работы в виртуальной среде должна поддерживать установку на следующие гипервизоры:

- VMware ESXi 6.7 Update 3.
- VMware ESXi 7.0 Update 3.
- VMware ESXi 8.0 Update 3.
- Microsoft Hyper-V Server 2019.
- Windows Server 2019 Standard с установленной ролью Hyper-V.
- Windows Server 2022 Standard с установленной ролью Hyper-V.
- РЕД Виртуализация 7.3

Система защиты веб-трафика должна обеспечивать защиту пользователей корпоративной сети при работе с веб-ресурсами: удалять вредоносные программы и другие программы, представляющие угрозу, из потока данных, поступающего в корпоративную сеть из интернета по протоколам HTTP(S) и FTP, блокировать зараженные и фишинговые веб-сайты, а также контролировать доступ к веб-ресурсам на основании категорий веб-ресурсов и типов контента и обеспечивать следующие функциональные возможности:

- выполнять антивирусную проверку объектов, передаваемых через прокси-сервер.
- лечить обнаруженные зараженные объекты и, если лечение невозможно, запрещать доступ к объекту.
- обнаруживать и лечить вирусы в любых типах файлов и вложений.
- блокировать вредоносные и фишинговые веб-сайты.
- использовать дополнительный уровень проверки на основе репутационных облачных сервисов производителя антивирусных средств защиты для обеспечения более высокой скорости реакции на угрозы, не дожидаясь обновления баз программы, а также снижения вероятности ложных срабатываний.
- осуществлять контроль и защиту SSL-шифрованного сетевого трафика при замене сертификата на стороне встроенного или внешнего прокси-сервера.
- настраивать правила доступа и защиты на основании следующих критериев:
    1. Категория веб-сайта
    2. URL ресурса
    3. Имя файла
    4. Тип файла
    5. Размер файла
    6. MIME-тип
    7. Хеш-сумма файла (MD5, SHA256)
    8. Направление трафика
    9. HTTP-метод
    10. HTTP Content-Length
    11. LDAP-запись
    12. User-agent
    13. IP-адрес или маска подсети
- настраивать приоритет выполнения прав доступа и защиты
- выполнять контроль доступа пользователей к Интернет-ресурсам на основании категорий веб-сайтов и типов контента, определенных производителем средства защиты.
- поддержка в качестве фильтра URL-адресов масок и регулярных выражений.
- осуществлять контроль использования пользователями только определенного типа веб-обозревателя (блокирование запрещенных в управляемых организациях браузер-клиентов).
- осуществлять настройку временного расписания правил контроля доступа пользователей к Интернет-ресурсам.
- интегрироваться с Microsoft Active Directory для назначения ролей пользователям управляющей консоли.
- обеспечивать возможность интеграции с несколькими доменами Microsoft Active Directory.
- обеспечивать поддержку NTLM- и Kerberos-аутентификации для службы единого входа (Single Sign-On).
- осуществлять поддержку рабочих областей для выделенных групп на основании сетевых адресов, масок подсетей, LDAP-записей.
- настраивать индивидуальные правила обработки и проверки трафика для рабочих областей, а также права доступа для администраторов этих организаций.

- возможность настраивать внешний вид страницы блокировки отдельно для каждой рабочей области
- настраивать вид веб-страницы, информирующей пользователя о блокировке Интернет-ресурса.
- вести статистику работы, включающую в себя помимо прочего информацию о выполнении и результатах антивирусной проверки, ошибках в работе приложения и предупреждениях.
- позволять экспортировать журналы событий программы в формат CSV.
- расследовать инциденты доступа в интернет с помощью поиска и просмотра событий.
- карточка события помимо прочего должна включать в себя:
    1. URL
    2. протокол
    3. домен
    4. результат детектирования технологиями защиты
    5. время наступления события
    6. имя пользователя
    7. User Agent пользователя
    8. IP-адрес пользователя
    9. категорию, к которой относится веб-ресурс
- публиковать события программы в систему корреляции событий (SIEM) по протоколу Syslog. При этом информация о каждом событии должна передаваться как отдельное syslog-сообщение в формате CEF.
- обеспечивать возможность сбора диагностической информации о программе через веб-интерфейс
- настраивать параметры программы и управлять программой через веб-интерфейс
- поддерживать возможность импортировать и экспортировать значения параметров программы
- получать статистику работы программы по протоколу SNMP, включать и отключать отправку SNMP-ловушек
- осуществлять мониторинг состояния работы программы, сетевого трафика, обрабатываемого программой, количества проверенных и обнаруженных объектов, последних и наиболее часто встречающихся угроз, заблокированных пользователей и URL-адресов через web-интерфейс программы
- обновлять антивирусные базы, как с сайта компании – производителя (по защищенному и незащищенному http-протоколу), так и из настраиваемых ресурсов (HTTP- и FTP-серверов) по расписанию или по требованию.
- настраивать параметры прокси-сервера через веб-интерфейс программы (при развертывании из iso-файла)
- возможность группировать созданные правила доступа и защиты
- создавать правила обхода для веб-ресурсов, не требующих обработки механизмами защиты и контроля доступа
- возможность задать правила защиты по умолчанию
- возможности управления встроенным прокси-сервером через веб интерфейс программы

- подключение доверенных балансировщиков нагрузки с поддержкой заголовков PROXY protocol и HTTP Forwarded
- аутентификация пользователей на прокси сервере с использованием Kerberos и NTLM
- возможность осуществлять дешифрацию HTTPS трафика с использованием самоподписанного или корпоративного сертификата
- возможность создавать правила дешифрации трафика, в том числе для исключения ресурсов по IP и доменным именам из правил дешифрации
- возможность добавления отпечатков доверенных сертификатов в хранилище системы
- возможность управления форматом хранения журнала работы прокси-сервера
- возможность кластеризации решения
- возможность централизованного управления и мониторинга серверов системы, собранных в кластер
- должна поддерживаться возможность интеграции с системами типа «песочница» для отправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования
- возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF.

Требования к программным средствам антивирусной защиты и фильтрации спама с помощью отдельного сервера

Система должна поставляться в виде:

1. ISO-образа, с предустановленной операционной системой, почтовым-сервером и средствами защиты почтового трафика на базе операционной системы Rocky Linux 9.8. Операционная система Rocky Linux 9.8 входит в состав образа системы.
2. ISO-образа, с предустановленной операционной системой, почтовым-сервером и средствами защиты почтового трафика на базе операционной системы РЕД ОС 8.0 из образа redos-8-20250711.7-Everything-x86_64-DVD1.iso.

-

Система должна поддерживать установку на физический и виртуальный сервер, для работы в виртуальной среде должна поддерживать установку на следующие гипервизоры:

1. VMware ESXi 7.0 Update 3;
2. VMware ESXi 8.0 Update 3;
3. Microsoft Hyper-V Server 2019;
4. Microsoft Hyper-V Server 2022;
5. Windows Server 2019 Standard с ролью Hyper-V;
6. Windows Server 2022 Standard с ролью Hyper-V;
7. РЕД Виртуализация 7.3.0;
8. РЕД Виртуализация 7.3.3;

9. Гипервизор на базе Astra Linux Special Edition 1.8.3 под управлением VMmanager 2026.01.1-1

Программные средства антивирусной защиты и фильтрации спама должны обеспечивать реализацию следующих функциональных возможностей:

- поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
- проверка входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговых рассылок), удаление выявленных сообщений, помещение копии сообщений в карантин;
- наличие общего карантина сообщений;
- управление карантином из веб-интерфейса;
- детектирование вредоносных и фишинговых ссылок в теле письма, включая ссылки, извлечённые из QR-кодов в графических вложениях;
- наличие эвристических методов детектирования;
- возможность включить или отключить добавление информационных заголовков в начало сообщения и в MIME-часть сообщения;
- возможность проверки получателей сообщений согласно списку допустимых получателей, наполняемому вручную или при интеграции с LDAP;
- возможность экспорта параметров приложения в зашифрованном виде;
- возможность просмотра содержимого сообщения в веб-интерфейсе продукта;
- возможность использования репутационных облачных сервисов;
- возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
- наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
- обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов, блокировать отдельные файлы;
- выполнять контентную фильтрацию сообщений по имени (в том числе внутри архивов и составных объектов), размеру и типу вложений, заголовкам, теме и телу письма, определять формат и тип вложения независимо от его расширения, удалять сообщения, содержащие вложения определённого формата или с определённым именем, или сообщения, размер которых превышает допустимый, помещать копии сообщений в хранилище;
- сохранять резервные копии сообщений в карантине по результатам их обработки модулями защиты;
- сохранять сообщения из карантина в файл и пересылать сообщения получателям;

- поддержка развёртывания кластерной архитектуры с централизованным управлением и возможностью балансировки входящего почтового трафика между несколькими серверами с настройкой приоритетов как глобально, так и для отдельных доменов;
- интеграция со службами каталогов Active Directory, включая поддержку многоуровневых лесов Active Directory (forest-wide), ALD Pro;−
- возможность отправки ловушек по протоколу SNMP, включая расширенные счётчики по карантину спама, карантину целевых атак и статистике сканирования (в т.ч. количество обнаруженных/необнаруженных угроз, ошибки сканирования, таймауты);
- обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей;
- возможность клонирования правил и изменения их приоритета путём перетаскивания в списке;
- при настройке правил должна быть возможность добавлять примечания к сообщению не только по результату срабатывания правила, но и по результату работы каждого модуля защиты отдельно;
- отправлять уведомления пользователям о результатах проверки их сообщений модулями программы;
- поддерживать работу персонального карантина на основе LDAP-записей;
- доступ к персональному карантину должен осуществляться на основе учетных записей LDAP;
- отправлять уведомления пользователям о состоянии персонального карантина, уведомления должны содержать список последних сообщений в карантине;
- настройки расписания отправки уведомлений;
- возможность почтовой рассылки с информацией о последних сообщениях, помещенных в персональное хранилище пользователя, с возможностью выполнения разрешенных действий над сообщениями, как из персонального хранилища, так и непосредственно из почтового уведомления;
- обеспечивать возможность повторной проверки почтовых сообщений технологиями защиты перед их отправкой из Хранилища;
- поддержка автоматического поиска пароля от зашифрованного вложения в теле самого сообщения;
- обеспечивать возможность автоматического поиска паролей в тексте почтового сообщения и их использования для проверки защищенных паролем документов Microsoft Office, содержащихся во вложениях;
- обновлять базы программы с серверов обновлений и пользовательских ресурсов (HTTP-, HTTPS- и FTP-серверов, локальных и сетевых папок) по расписанию и по требованию;
- отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования;
- настраивать режимы TLS-шифрования сообщений для ситуаций, когда система принимает сообщения от другого сервера (действует как Сервер) или пересылает сообщения на другой сервер (действует как Клиент), а также настраивать параметры TLS для отдельных доменов;

- осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC, причём каждая технология должна быть настраиваема как отдельное условие в выражениях фильтрации;
- подписывать исходящие сообщения электронной почты с помощью технологии DKIM;
- возможность для каждого статуса проверок SPF и DMARC задать отдельное действие над сообщением и настроить уведомления по результатам каждой проверки;
- осуществлять проверку подлинности отправителей сообщений с помощью технологии сопоставления доменов отправителя;
- возможность публикации событий в SIEM-систему с настройкой при помощи веб-интерфейса;
- добавлять предупреждения о небезопасном вложении к входящим сообщениям в теме письма;
- просматривать журнал событий, аудита в веб интерфейсе программы и загружать его на жесткий диск;
- фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- проверка совпадения доменов отправителя сообщения, указанных в SMTP-сессии (значение команды MAIL FROM) и в сообщении (значение MIME-заголовка From);
- проверка корректности синтаксиса адресов отправителей и получателей в SMTP-сессии на соответствие стандарту RFC;
- проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
- выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
- перенос в карантин зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка;
- использование регулярных выражений при создании правил фильтрации;
- в правилах фильтрации сообщений электронной почты указывать пользователей и группы пользователей из Microsoft Active Directory;
- наличие встроенных ролей администратора и специалиста поддержки;
- возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты;
- управление работой программы должно осуществлять как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Mozilla Firefox версии 127.0.2. или выше, Google Chrome версии 129.0.6668 или выше, Microsoft Edge версии 129.0.2792 или выше;
- должна поддерживаться возможность интеграции с системами типа «песочница» для отправки файлов на анализ, при этом каждому сообщению должен присваиваться уникальный идентификатор (UUID), а в песочницу передаваться список получателей и результаты проверки по каждому модулю;
- возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF;

- обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга считать сообщение спамом.
- возможность управления маршрутизацией почтового трафика через веб-интерфейс, включая маршрутизацию почтовых сообщений на основании имени и значения их заголовков;
- должен быть доступен мастер первоначальной настройки для быстрой конфигурации MTA и сетевых параметров после развёртывания виртуальной машины;
- настраивать режимы TLS-шифрования сообщений для ситуаций, когда система принимает сообщения от другого сервера (действует как Сервер) или пересылает сообщения на другой сервер (действует как Клиент), а также настраивать параметры TLS для отдельных доменов.
- выявлять почтовые сообщения с нарушенной или некорректной структурой, в том числе сообщения, намеренно модифицированные с целью реализации атаки либо сформированные некорректно вследствие ошибок программного обеспечения, с возможностью настройки действий над такими сообщениями;
- выполнять репутационную проверку IP-адресов и доменов отправителей с учетом технической информации о маршруте прохождения почтового сообщения, содержащейся в его служебных заголовках;
- обеспечивать возможность централизованного удаления заданных заголовков из почтовых сообщений до применения правил их обработки;
- обеспечивать возможность поиска и фильтрации правил обработки почтовых сообщений по их параметрам, а также добавления комментариев к спискам отправителей и получателей, используемым в правилах;
- просматривать системные журналы непосредственно через веб-интерфейс;
- записывать в журнал подробную информацию о срабатывании правил контентной фильтрации, включая анализ до 10 MIME-частей сообщения;
- управление работой программы должно осуществляться через веб-интерфейс, обеспечивающий настройку MTA, маршрутизации, DKIM и TLS-ключей, доменов и адресов;
- обеспечивать формирование и отображение статистической информации о пользователях, наиболее часто получавших опасные почтовые сообщения, включая сообщения с вредоносным, фишинговым и спам-содержимым, за выбранный период времени;
- обеспечивать возможность автоматического выявления паролей в тексте почтового сообщения и их использования для проверки защищенных паролем документов Microsoft Office, содержащихся во вложениях.

Требования к программным средствам антивирусной защиты и фильтрации спама для почтовых серверов, установленных на операционную систему семейства Linux

Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:

1. Rocky Linux 9.7, 10.1;

2. Ubuntu 22.04 LTS, 24.04 LTS;
3. Red Hat Enterprise Linux 9.7, 10.1;
4. Debian 12.13, 13.3;
5. РЕД ОС 7.3 (только из образа redos-MUROM-7.3-20241221.0-Everything-x86_64-DVD1.iso);
6. РЕД ОС 8.0 (только из образа redos-8-20250711.7-Everything-x86_64-DVD1.iso);
7. Astra Linux Special Edition 1.7 (уровень защиты «Смоленск»), с обновлением 1.7.9, БЮЛЛЕТЕНЬ № 2025-1202SE17, ядро generic;
8. Astra Linux Special Edition 1.8 (уровень защиты «Смоленск»), с обновлением 1.8.4, БЮЛЛЕТЕНЬ № 2025-1113SE18, ядро generic;

Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать совместно с почтовыми системами следующих версий:

1. Exim- 4.92 и выше.
2. Postfix- 3.5.25 и выше.

Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать совместно с веб-сервером Nginx версии 1.18.1. и выше. При использовании системы под управлением Astra Linux Special Edition требуется веб-сервер Apache минимальной версии 2.4.62.

Программные средства антивирусной защиты и фильтрации спама должны обеспечивать реализацию следующих функциональных возможностей:

- поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
- проверка входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговых рассылок), удаление выявленных сообщений, помещение копии сообщений в карантин;
- наличие общего карантина сообщений;
- управление карантином из веб-интерфейса;
- детектирование вредоносных и фишинговых ссылок в теле письма, включая ссылки, извлечённые из QR-кодов в графических вложениях;
- наличие эвристических методов детектирования;
- возможность включить или отключить добавление информационных заголовков в начало сообщения и в MIME-часть сообщения;
- возможность проверки получателей сообщений согласно списку допустимых получателей, наполняемому вручную или при интеграции с LDAP;
- возможность экспорта параметров приложения в зашифрованном виде;
- возможность просмотра содержимого сообщения в веб-интерфейсе продукта;
- возможность использования репутационных облачных сервисов;
- возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
- наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;

- обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов, блокировать отдельные файлы;
- выполнять контентную фильтрацию сообщений по имени (в том числе внутри архивов и составных объектов), размеру и типу вложений, заголовкам, теме и телу письма, определять формат и тип вложения независимо от его расширения, удалять сообщения, содержащие вложения определённого формата или с определённым именем, или сообщения, размер которых превышает допустимый, помещать копии сообщений в хранилище;
- сохранять резервные копии сообщений в карантине по результатам их обработки модулями защиты;
- сохранять сообщения из карантина в файл и пересылать сообщения получателям;
- интеграция со службами каталогов Active Directory, включая поддержку многоуровневых лесов Active Directory (forest-wide), ALD Pro;
- возможность отправки ловушек по протоколу SNMP, включая расширенные счётчики по карантину спама, карантину целевых атак и статистике сканирования (в т.ч. количество обнаруженных/необнаруженных угроз, ошибки сканирования, таймауты);
- обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей;
- отправлять уведомления пользователям о результатах проверки их сообщений модулями программы;
- поддерживать работу персонального карантина на основе LDAP-записей;
- доступ к персональному карантину должен осуществляться на основе учетных записей LDAP;
- отправлять уведомления пользователям о состоянии персонального карантина, уведомления должны содержать список последних сообщений в карантине;
- настройки расписания отправки уведомлений;
- возможность почтовой рассылки с информацией о последних сообщениях, помещенных в персональное хранилище пользователя, с возможностью выполнения разрешенных действий над сообщениями, как из персонального хранилища, так и непосредственно из почтового уведомления;
- обеспечивать возможность повторной проверки почтовых сообщений технологиями защиты перед их отправкой из Хранилища;
- обеспечивать возможность ввода пользователем паролей от зашифрованных объектов при отправке почтовых сообщений из персонального Хранилища для использования указанных паролей при повторной проверке сообщений;
- поддержка автоматического поиска пароля от зашифрованного вложения в теле самого сообщения;

- обеспечивать возможность автоматического поиска паролей в тексте почтового сообщения и их использования для проверки защищенных паролем документов Microsoft Office, содержащихся во вложениях;
- обновлять базы программы с серверов обновлений и пользовательских ресурсов (HTTP-, HTTPS- и FTP-серверов, локальных и сетевых папок) по расписанию и по требованию;
- отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования;
- настраивать режимы TLS-шифрования сообщений для ситуаций, когда система принимает сообщения от другого сервера (действует как Сервер) или пересылает сообщения на другой сервер (действует как Клиент), а также настраивать параметры TLS для отдельных доменов;
- осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC, причём каждая технология должна быть настраиваема как отдельное условие в выражениях фильтрации;
- подписывать исходящие сообщения электронной почты с помощью технологии DKIM;
- добавлять предупреждения о небезопасном вложении к входящим сообщениям в теме письма;
- просматривать журнал событий и аудита в веб-интерфейсе программы и загружать его на жёсткий диск;
- просматривать системные журналы непосредственно через веб-интерфейс;
- записывать в журнал подробную информацию о срабатывании правил контентной фильтрации, включая анализ до 10 MIME-частей сообщения;
- фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- проверка совпадения доменов отправителя сообщения, указанных в SMTP-сессии (значение команды MAIL FROM) и в сообщении (значение MIME-заголовка From);
- проверка корректности синтаксиса адресов отправителей и получателей в SMTP-сессии на соответствие стандарту RFC;
- проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
- выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
- перенос в карантин зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка;
- использование регулярных выражений при создании правил фильтрации;
- в правилах фильтрации сообщений электронной почты указывать пользователей и группы пользователей из Microsoft Active Directory;
- наличие встроенных ролей администратора и специалиста поддержки;
- возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты;
- управление работой программы должно осуществляться как стандартными средствами операционной системы с помощью командной строки, так и через

специальный веб-интерфейс, работающий на браузерах: Mozilla Firefox версии 127.0.2 или выше, Google Chrome версии 139.0.7258 или выше, Microsoft Edge версии 139.0.3405 или выше;

- должна поддерживаться возможность интеграции с системами типа «песочница» для отправки файлов на анализ, при этом каждому сообщению должен присваиваться уникальный идентификатор (UUID), а в песочницу передаваться список получателей и результаты проверки по каждому модулю;
- возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF;
- обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга считает сообщение спамом.
- выявлять почтовые сообщения с нарушенной или некорректной структурой, в том числе сообщения, намеренно модифицированные с целью реализации атаки либо сформированные некорректно вследствие ошибок программного обеспечения, с возможностью настройки действий над такими сообщениями;
- выполнять репутационную проверку IP-адресов и доменов отправителей с учетом технической информации о маршруте прохождения почтового сообщения, содержащейся в его служебных заголовках;
- обеспечивать возможность централизованного удаления заданных заголовков из почтовых сообщений до применения правил их обработки;
- обеспечивать возможность поиска и фильтрации правил обработки почтовых сообщений по их параметрам, а также добавления комментариев к спискам отправителей и получателей, используемым в правилах;
- поддержка развёртывания в кластерной конфигурации с централизованным управлением (для горизонтального и вертикального масштабирования);
- возможность клонирования правил и изменения их приоритета путём перетаскивания в списке;
- при настройке правил должна быть возможность добавлять примечания к сообщению не только по результату срабатывания правила, но и по результату работы каждого модуля защиты отдельно;
- возможность публикации событий в SIEM-систему с настройкой при помощи веб-интерфейса;
- обеспечивать формирование и отображение статистической информации о пользователях, наиболее часто получавших опасные почтовые сообщения, включая сообщения с вредоносным, фишинговым и спам-содержимым, за выбранный период времени;
- обеспечивать возможность автоматического выявления паролей в тексте почтового сообщения и их использования для проверки защищенных паролем документов Microsoft Office, содержащихся во вложениях.

Требования к программным средствам антивирусной защиты и фильтрации спама для серверов Microsoft Exchange

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

1. Microsoft Windows Server 2022 Standard или Datacenter;
2. Microsoft Windows Server 2019 Standard или Datacenter;
3. Microsoft Windows Server 2016 Standard или Datacenter.

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать с программным обеспечением Microsoft Exchange Server следующих версий:

1. Microsoft Exchange Server 2019, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
2. Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
3. Microsoft Exchange Server 2013 SP1, развернутый как минимум в одной из следующих ролей: Почтовый ящик, Пограничный транспорт или Сервер клиентского доступа (CAS).

Консоль управления программными средствами антивирусной защиты для серверов Microsoft Exchange должна быть реализована с использованием Microsoft Management Console и должна функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

1. Microsoft Windows Server 2022 Standard или Datacenter;
2. Microsoft Windows Server 2019 Standard или Datacenter;
3. Microsoft Windows Server 2016 Standard или Datacenter;
4. Операционные системы Microsoft Windows Server в режиме Core.
5. Microsoft Windows 11 (x64);
6. Microsoft Windows 10 (x64).

Для установки любого компонента программы (Сервера безопасности или Консоли управления) требуется пакет обновлений Microsoft Windows KB2999226.

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей:

- совместимость с DAG в Microsoft Exchange;
- поиск и удаление по требованию всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;

- поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в хранящихся на сервере Microsoft Exchange (в том числе в общих папках) сообщениях, включая вложения;
- наличие эвристических методов детектирования;
- проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер;
- возможность лечить зараженные архивы;
- возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях;
- возможность детектирования вредоносных и фишинговых ссылок в теле письма;
- сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта;
- набор параметров поиска для удобства нахождения объекта в резервном хранилище;
- дополнительный уровень проверки с помощью репутационных облачных сервисов;
- возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
- наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
- возможность проверять текст в сообщениях и в темах сообщений электронной почты на наличие запрещенных слов.
- проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения;
- защита от спуфинга (подделка адреса отправителя с целью сокрытия истинного автора сообщения электронной почты).
- фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
- использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и файлов вложений);
- возможность использовать роли пользователей/администраторов для разграничения доступа к настройкам безопасности;
- аудит изменения параметров программы по событиям в журнале событий Windows;
- мониторинг состояния программы, получение статистики работы программы и управление белыми и черными списками адресов Анти-Спама с помощью команд в среде Windows PowerShell;
- использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и имён файлов);
- возможность фильтрации файлов Microsoft Office, содержащих макросы;
- возможность проверки и удаления сообщений, являющихся спамом или содержащих фишинговые и вредоносные ссылки;

- проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
- создание отчетов по работе системы защиты;
- возможность автоматической рассылки отчетов администраторам по расписанию;
- возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации;
- возможность фоновой проверки почтовых ящиков и общих папок с использованием Exchange Web Services;
- детальные отчеты в формате HTML;
- наличие возможности отправки отчётов и уведомлений на указанные адреса электронной почты;
- мониторинг работы программы с помощью System Center - Operations Manager;
- интеграция с Active Directory;
- централизованный просмотра состояния защиты;
- возможность распределять роли администраторов системы.

Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

1. Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.
2. Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSB) 64-разрядная.
3. Windows Server 2019 Standard/Datacenter/Core 64-разрядная.
4. Windows Server 2022 Standard/Datacenter/Core 64-разрядная.
5. Windows Server 2025 Standard/Datacenter/Core 64-разрядная.
6. Windows Storage Server 2019 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

1. VMware vSphere 6.7.
2. VMware vSphere 7.0.
3. Microsoft Hyper-V Server 2019 64-разрядная.
4. Microsoft Hyper-V Server 2022 64-разрядная.
5. Citrix XenServer 7.1 LTSR.
6. Citrix XenServer 8.x.
7. Parallels Desktop 18.
8. Oracle VM VirtualBox 7.x.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

1. Microsoft SQL Server 2016 (все редакции) 64-разрядная.
2. Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная.
3. Microsoft SQL Server 2019 (все редакции) для Windows/Linux 64-разрядная (требуются дополнительные действия).
4. Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная.
5. MySQL 5.7 Community 32-разрядная/64-разрядная.
6. MySQL 8.0 Community 32-разрядная/64-разрядная.
7. MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
8. MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища Inno DB.
9. PostgreSQL 13.x 64-разрядная.
10. PostgreSQL 14.x 64-разрядная.
11. PostgreSQL 15.x 64-разрядная.
12. Postgres Pro 13.x Windows/Linux 64-разрядная.
13. Postgres Pro 14.x Windows/Linux 64-разрядная.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
- чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
- настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
- автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
- централизованные установка, обновление и удаление программных средств антивирусной защиты;
- централизованная настройка, администрирование;
- просмотр отчетов и статистической информации по работе средств защиты;
- централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
- сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
- наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
- указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
- иерархии триггеров, по которым происходит перераспределение;
- тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;

- доставка обновлений на рабочие места пользователей сразу после их получения;
- распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
- построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
- поддержка мультиарендности (multi-tenancy) для серверов управления;
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
- доступ к облачным серверам производителя антивирусного ПО через сервер управления;
- автоматическое распространение лицензии на клиентские компьютеры;
- инвентаризация установленного ПО и оборудования на компьютерах пользователей;
- наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
- функция управления мобильными устройствами через сервер iOS MDM;
- отправки SMS-оповещений о заданных событиях;
- централизованная установка сертификатов на управляемые мобильные устройства;
- указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
- указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
- построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
- наличие преднастроенных стандартных отчетов о работе системы;
- экспорт отчетов в файлы форматов PDF и XML;
- централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
- создание внутренних учетных записей для аутентификации на сервере управления;
- создание резервной копии системы управления встроенными средствами системы управления;
- поддержка Windows Failover Clustering;
- поддержка интеграции с Windows сервисом Certificate Authority;
- наличие портала самообслуживания пользователей;
- портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
- наличие системы контроля возникновения вирусных эпидемий;
- установки в облачной инфраструктуре Microsoft Azure и Google Cloud;

- интеграции по OpenAPI;
- управления антивирусной защитой с использованием WEB консоли;
- возможность управления развертыванием ОС Windows через консоль управления;
- наличие преднастроенных ролей пользователей средств централизованного управления;
- должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
- возможность подключения по RDP или штатными средствами из консоли управления;
- наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing);
- пользователю должен выводиться запрос на разрешение дистанционного подключения;
- наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal);
- должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
- возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС;
- возможность импортировать образ операционной системы из дистрибутивов (WIM)
- наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;
- автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры;
- поддержка функциональности управления шифрованием данных;
- возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF
- двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
- использования дополнительной аутентификация после изменения параметров учетной записи пользователя.
- возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами.
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей и серверах под управлением Mi crosoft Windows;
- возможность развернуть Сервер администрирования как систему высокой доступности;
- возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети;
- удаленная диагностика клиентских устройств на базе Windows и Linux (получение трассировок, журналов событий, дампов, остановка и запуск приложений);

- возможность отозвать права локального администратора учетных записей на управляемых устройствах с операционной системой Linux;
- возможность изменить пароль локальной учетной записи на управляемых устройствах с операционной системой Linux.

Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

1. Debian GNU/Linux 12 (Bookworm) 64-разрядная.
2. Debian GNU/Linux 13 (Trixie) 64-разрядная.
3. Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
4. Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.
5. CentOS Stream 9 64-разрядная.
6. CentOS Stream 10 64-разрядная.
7. Red Hat Enterprise Linux Server 7.x 64-разрядная.
8. Red Hat Enterprise Linux Server 8.x 64-разрядная.
9. Red Hat Enterprise Linux Server 9.x 64-разрядная.
10. Red Hat Enterprise Linux Server 10.x 64-разрядная.
11. SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
12. SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
13. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
14. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
15. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная.
16. Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная.
17. Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная.
18. Astra Linux Special Edition RUSB.10015-03 (очередное обновление 7.6) 64-разрядная.
19. Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная.
20. Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
21. Альт СП Сервер 10 64-разрядная.
22. Альт СП Рабочая станция 10 64-разрядная.
23. Oracle Linux 7 64-разрядная.
24. Oracle Linux 8 64-разрядная.
25. Oracle Linux 9 64-разрядная.
26. Platform V SberLinux OS Server (SLO) 8.10.1 64-разрядная.
27. Platform V SberLinux OS Server (SLO) 9.5.1 64-разрядная.
28. Platform V SberLinux OS Server (SLO) 9.6 64-разрядная.
29. РЕД ОС 7.3 Сервер 64-разрядная.
30. РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
31. РЕД ОС 8 64-разрядная.
32. РОСА "КОБАЛЬТ" 7.9 64-разрядная.

33. M ОС (Moscow Electronic School) 12 Сервер 64-разрядная.
34. Mostech Server 64-разрядная.
35. МосОС 15.5 Arbat 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

1. VMware vSphere 6.7.0.
2. VMware vSphere 7.0.3.
3. Microsoft Hyper-V Server 2019 64-разрядная.
4. Microsoft Hyper-V Server 2022 64-разрядная.
5. Citrix XenServer 7.x.
6. Citrix XenServer 8.2.
7. Parallels Desktop 18.
8. Oracle VM VirtualBox 7.0.12.
9. Kernel-based Virtual Machine (все поддерживаемые ОС Linux).

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

1. MySQL 5.7 Community 32-разрядная/64-разрядная.
2. MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
3. MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
4. MySQL Standard Edition 8.4 32-разрядная/64-разрядная.
5. MySQL Enterprise Edition 8.4 32-разрядная/64-разрядная.
6. MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
7. MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
8. MariaDB 10.4 (сборка 10.4.20 и выше) 32-разрядная/64-разрядная.
9. MariaDB 10.5 (сборка 10.5.27 и выше) 32-разрядная/64-разрядная.
10. MariaDB 10.6 (сборка 10.6.20 и выше) 32-разрядная/64-разрядная.
11. MariaDB 10.11 (сборка 10.11.10 и выше) 32-разрядная/64-разрядная.
12. MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
13. PostgreSQL 13.x 64-разрядная.
14. PostgreSQL 14.x 64-разрядная.
15. PostgreSQL 15.x 64-разрядная.
16. PostgreSQL 15.x 64-разрядная (кластер Corosync/Pacemaker).
17. PostgreSQL 16.x 64-разрядная.
18. PostgreSQL 17 64-разрядная.
19. PostgreSQL 18 64-разрядная.
20. Postgres Pro 13.x (все редакции) 64-разрядная.
21. Postgres Pro 14.x (все редакции) 64-разрядная.
22. Postgres Pro 15.x (все редакции) 64-разрядная.
23. Postgres Pro 15.x 64-разрядная (кластер Corosync/Pacemaker).
24. Postgres Pro 16.x (все редакции) 64-разрядная.
25. Postgres Pro 16.x Enterprise 64-разрядная (кластер Built-in High Availability).

26. Postgres Pro 17 (все редакции) 64-разрядная.
27. Postgres Pro 17 Enterprise 64-разрядная (кластер Built-in High Availability).
28. Postgres Pro 18 (все редакции) 64-разрядная.
29. Postgres Pro 18 Enterprise 64-разрядная (кластер Built-in High Availability).
30. Platform V Pangolin 6.5.1 64-разрядная.
31. Platform V Pangolin 6.5.1 64-разрядная (кластер Built-in High Availability).
32. Jatoba 4 64-разрядная.
33. Jatoba 5 64-разрядная.
34. Tantor SE 1C 64-разрядная.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- централизованные установка, обновление и удаление программных средств антивирусной защиты;
- централизованная настройка, администрирование;
- просмотр отчетов и статистической информации по работе средств защиты;
- сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
- иерархии триггеров, по которым происходит перераспределение;
- доставка обновлений на рабочие места пользователей сразу после их получения;
- распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
- построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
- поддержка мультиарендности (multi-tenancy) для серверов управления;
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
- доступ к облачным серверам производителя антивирусного ПО через сервер управления;
- автоматическое распространение лицензии на клиентские компьютеры;
- наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
- построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
- наличие преднастроенных стандартных отчетов о работе системы;
- экспорт отчетов в файлы форматов PDF и XML;
- централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
- создание внутренних учетных записей для аутентификации на сервере управления;
- двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;

- создание резервной копии системы управления встроенными средствами системы управления;
- наличие системы контроля возникновения вирусных эпидемий;
- управления антивирусной защитой с использованием WEB консоли;
- обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
- с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
- использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули;
- возможность передачи ключей шифрования между серверами централизованного управления;
- выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных;
- возможность экспорта и импорта выборок событий;
- возможность экспорта событий в SIEM-систему в форматах CEF или LEEF;
- возможность управления мобильными устройствами на Android и iOS;
- получение информации о программах, установленных на управляемые устройства;
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей и серверах под управлением Mi crosoft Windows;
- возможность поиска устройств по контроллерам доменов Microsoft Active Directory и Samba;
- возможность автоматизированного переноса данных с сервера администрирования под управлением ОС Windows на сервер администрирования под управлением ОС Linux;
- возможность удалённой диагностики управляемых устройств;
- поддержка кластерной технологии;
- возможность централизованного удаления несовместимого ПО с управляемых устройств;
- возможность централизованной перезагрузки управляемых устройств;
- возможность задать профили соединения для автономных пользователей с Linux-устройствами для подключения к одному и тому же или разным серверам централизованного управления в зависимости от местоположения устройства;
- поддержка контроллеров домена FreeIPA и ALD Pro;
- поддержка доменной аутентификации по Kerberos (технология единого входа, в том числе на основе сертификатов).

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;
- множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
- проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации

- 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:

- Предоставляться на русском и казахском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Республики Казахстан по электронной почте и через Интернет.
- Web-сайт производителя антивирусного решения должен иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

По вопросам технической спецификации обращаться: Рязанов Д.В., тел. +7-727-244-52-73, e-mail: dim@kazrosgas.kz

Подписал	Рязанов Дмитрий Владимирович
Дата подписания	09.11.2026