Требования к продукту для Централизованного управления антивирусной защитой на 2000 персонального компьютера и серверного оборудования

Оглавление

Общие требования 2

Консоль (Сервер управления) 2

Защита рабочих станций 5

Защита серверов 10

Требования законодательства 13

Общие требования

1. Интерфейс программных продуктов, включая средства централизованного управления, должен быть на английском и русском языках.
2. Программные продукты, включая средства централизованного управления, должны обладать контекстной справочной системой на английском и русском языках.
3. Наличие эксплуатационной документации для программного продукта, включая средства централизованного управления, которые должны включать документы, подготовленные в соответствии с требованиями государственных стандартов, на английском и русском языках, в том числе «Руководство пользователя (администратора)».
4. Документация, поставляемая с программным продуктом, включая средства централизованного управления, должна детально описывать процесс установки, настройки и эксплуатации соответствующего программного продукта.
5. Техническая поддержка программного продукта, включая средства централизованного управления, должна предоставляться на русском и английском языках, сертифицированными специалистами производителя программного продукта по телефону, электронной почте и при необходимости с оперативным выездом к заказчику.
6. Web-сайт производителя программного решения должен быть на английском и русском языках, и иметь специальный раздел, посвящённый технической поддержке программного продукта, актуальную базу знаний, а также форум пользователей программных продуктов.

Консоль (Сервер управления)

1. Возможность централизованного управления антивирусной защитой всей сетевой инфраструктуры из единого веб-интерфейса.
2. Возможность построения иерархической структуры администрирования, которая состоит из главного сервера и подчиненных серверов, что дает возможность осуществлять централизованное управление антивирусной защитой рабочих станций, серверов и мобильных устройств, что принадлежат как главному, так и региональным подразделениям.
3. Инвентаризация оборудования, которое установлено на конечных устройствах и серверах под управлением Windows, macOS и Linux.
4. Инвентаризация программного обеспечения, которое установлено на рабочих станциях и серверах под управлением Windows, macOS и Linux.
5. Наличие инструмента для удаленной установки как различного пользовательского программного обеспечения, так и антивирусного программного обеспечения для операционных систем Windows, Linux и macOS на несколько конечных точек одновременно.
6. Наличие функционала для удаленной деинсталляции как пользовательского программного обеспечения, так и антивирусного программного обеспечения для операционных систем Windows, Linux и macOS.
7. Возможность выполнять с помощью инструмента удаленного управления дополнительные сетевые действия, такие как: завершение работы и перезагрузка, отправка сигнала пробуждения компьютера, отправка сообщений, выполнение конкретных инструкций командной строки на клиентском компьютере, старт обновления операционной системы клиентского компьютера.

8. Наличие инструмента для создания и редактирования установочных пакетов для операционных систем Windows, Linux и macOS с предварительно установленными настройками конфигурации, что позволяет экспортировать установочные пакеты для развертывания полноценной антивирусной защиты на конечных точках в изолированной сети, а также на конечных точках, которые нуждаются в защите, но временно не подключены к серверу администрирования.

9. Наличие диспетчера пользователей, который позволяет создавать пользователей сервера администрирования и назначать им разные права доступа к отдельным разделам, группам компьютеров на сервере администрирования, что дает возможность предоставить разные права доступа для региональных системных администраторов разветвленной системы антивирусной защиты.

10. Возможность аутентифицировать администраторов консоли управления с помощью групп безопасности Active Directory.

11. Возможность использования двухфакторной аутентификации для учетных записей администраторов, что позволяет предотвратить несанкционированное подключение к серверу централизованного управления.

12. Наличие журнала аудита, в котором регистрируются и отслеживаются все изменения в конфигурации и все действия, которые выполняют пользователи сервера администрирования.

13. Возможность удаленно активировать и деактивировать модули защиты, такие как персональный брандмауэр, защита в режиме реального времени, защита почтового клиента, защита доступа в Интернет, контроль устройств, веб-контроль, антиспам на отдельно взятом клиенте.

14. Возможность создавать и редактировать статические группы и возможность импорта из Active Directory дерева компьютеров.

15. Возможность настройки автоматического распределения клиентов по динамическим группам по многим критериям с последующим назначением соответствующих политик безопасности, а также запуском необходимых задач.

16. Возможность импорта пользователей и групп из Active Directory для дальнейшего использования их для персонализации правил контроля устройств и веб-контроля.

17. Возможность использовать как встроенные, так и пользовательские политики, предназначенные для постоянного обслуживания конфигурационных настроек антивирусных продуктов. Возможность осуществлять экспорт/импорт политик.

18. Наличие панели мониторинга, которая предоставляет всю необходимую подробную информацию относительно уровня защиты безопасности инфраструктуры, состояния защищенных конечных точек, а также состояния самого сервера администрирования.

19. Наличие не менее 100 предустановленных шаблонов отчетов, которые могут использоваться как для панели мониторинга, так и для формирования различных отчетов.

20. Возможность создавать и редактировать шаблоны отчетов, которые используются как для панели мониторинга, так и для формирования отчетов в форматах PDF, CSV и дальнейшего хранения по указанному пути или отправки на указанную электронную почту.

21. Поддержка интеграции с ведущими SIEM системами, такими как Microsoft Sentinel, Stellar Cyber, IBM QRadar, Wazuh, Elastic или Splunk.

22. Иметь возможность предоставить REST API сторонним SIEM системам для отправки запросов и получать соответствующие события безопасности и телеметрию напрямую.

23. Возможность экспортировать журналы в syslog для дальнейшей интеграции с SIEM.

24. Возможность настраивать параметры журналов и отчетов или выбрать из более чем 50 шаблонов для различных систем/клиентов.

25. Возможность создавать зеркало обновлений с помощью антивирусного продукта, специальной утилиты или прокси сервера.

26. Возможность создания зеркала обновлений на основе сторонних HTTP-серверов.

27. Веб-ориентированный интерфейс, который дает возможность управлять сервером через любой браузер путем соединения, защищенного сертификатом.

28. Использование независимого агента, который позволяет осуществлять удаленное управление антивирусным продуктом на конечных точках, а также контролировать уровень антивирусной защиты на рабочих станциях и состояние операционной системы.

29. Модуль агента управления должен:

– распространяться в виде облегченного ядра (без предустановленных функциональных модулей);

– поддерживать подгрузку функциональных модулей с сервера управления на основе активированных политик и включенных защитных функций;

– обеспечивать двусторонний режим обмена данными с сервером управления;

– поддерживать управление из командной строки;

– иметь встроенные механизмы самозащиты, отключаемые только через централизованную панель управления посредством политик с использованием пароля;

– поддерживать установку без первичной привязки к серверу управления (в целях использования в шаблонах и установочных образах);

– поддерживать привязку к серверу управления с использованием инструментов командной строки;

– поддерживать использование инструментов командной строки для настройки агента;

– поддерживать актуальные версии серверных и клиентских операционных систем Windows и дистрибутивов Linux, входящие в текущий жизненный цикл поддержки производителя.

30. Возможность отслеживать установленное на рабочей станции ПО и управлять его состоянием, а также удалять установленное ПО на выбор.

31. Иметь дополнительный компонент, что позволяет управлять антивирусной защитой на мобильных устройствах.

32. Специальный компонент, который осуществляет обнаружение в сети незащищенных рабочих станций для дальнейшего развертывания на них антивирусной защиты.

33. Защита соединений между компонентами сервера с помощью как самостоятельно выпущенных сертификатов, так и существующих сертификатов.

34. Наличие запатентованной технологии с функцией автоматического восстановления зашифрованных файлов при обнаружении программ-вымогателей (ransomware) на поздних этапах атаки, после того как процесс шифрования уже начался и дополняющую существующую функцию Ransomware Shield.

35. Инструмент для управления состоянием лицензий (даже без использования сервера администрирования).

36. Возможность деактивировать лицензию антивирусных продуктов даже на рабочих станциях, к которым нет физического или удаленного доступа.

37. Возможность определять, какая виртуальная машина будет являться источником для копирования или клонирования в системах VDI.

38. Наличие мастера настройки для определения подробных параметров для интеграции с системами VDI.

39. Возможность выбирать варианты обработки идентификаторов клонированных компьютеров, такие как сопоставление существующими компьютерами или создание новых компьютеров.

40. Возможность определять параметры шаблона именования VDI для мгновенных клонов или каталогов машин.

41. Наличие предустановленных шаблонов в системе уведомлений для информирования о некорректной идентификации клонированных машин, что дает возможность оповещать о некорректно настроенной интеграции с системами VDI.

42. Наличие автоматического обновления агента управления, что дает возможность без вмешательства администраторов использовать актуальные версии.

43. Наличие механизма распределения автоматического процесса обновления, что дает возможность снизить нагрузку на сеть и компьютеры в целом.

44. Возможность установки агента управления на ARM64 процессорах.

45. Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам.

46. Наличие функционала для определения администратора площадки или филиала с соответствующей частью лицензии.

47. Поддержка ОС агентом управления: Microsoft Windows 10 / 11; Red Hat Enterprise Linux (RHEL) 8 / 9; CentOS 7.9; Ubuntu Desktop 20.04 LTS / 22.04 LTS / 24.04 LTS; Debian 11 / 12; SUSE Linux Enterprise Server (SLES) 15; Oracle Linux 8 / 9; Amazon Linux 2 / 2023; Alma Linux 8 / 9; Rocky Linux 8 / 9; Linux Mint 20 / 21 / 22; macOS 11 / 12 / 13 14 / 15 / 26.

Защита рабочих станций

1. Предоставление защиты от вирусов, троянского ПО, рекламного ПО, фишинга, а также шпионского ПО.

2. Предоставление защиты от вредоносного ПО – определенного вредоносного кода, который добавляется в начало или конец кода файлов на компьютере. Выявление вредоносного ПО должно осуществляться ядром обнаружения в сочетании с компонентом машинного обучения.

3. Предоставление защиты от потенциально нежелательных программ, которые нельзя однозначно отнести к вредоносному ПО, по аналогии с такими безусловно вредоносными программами, как вирусы или трояны, но эти программы могут устанавливать дополнительное нежелательное ПО, менять настройки системы, а также выполнять неожиданные действия или действия, не подтвержденные пользователем.

4. Предоставление защиты от потенциально опасных программ – разнообразного ПО, которое может использоваться для вредоносных целей, таких как несанкционированный удаленный доступ, кража или взлом паролей, клавиатурные шпионы и другие.

5. Предоставление защиты от подозрительных программ – программ, которые сжатые упаковщиками или протекторами, которые часто используют злоумышленники для предотвращения обнаружения вредоносного программного обеспечения.

6. Предоставление защиты от опасных программ руткитов, которые предоставляют злоумышленникам из Интернета неограниченный доступ к системе, в то же время скрывая свое присутствие в операционной системе.

7. Возможность для различных категорий угроз настраивать отдельные уровни реагирования как для защиты, так и для отчетности.

8. Возможность делать исключения из сканирования определенных файлов, которые не вредоносные, но сканирование которых может привести к отклонениям в работе или влиять на продуктивность системы.

9. Возможность создания исключений для общесистемных процессов с целью улучшить скорость работы системных служб и минимизировать вмешательство в процесс работы ОС.

10. Возможность осуществлять проверку загрузочных секторов на наличие вирусов в главной загрузочной записи, в том числе интерфейса UEFI.

11. Обеспечение антивирусной защиты в режиме реального времени.

12. Использование эвристических технологий собственной разработки во время сканирования.

13. Наличие инструмента антивирусного сканирования по требованию пользователя или администратора и в соответствии с графиком.

14. Модуль защиты документов, который должен давать возможность проверять макросы Microsoft Office на наличие вредоносного кода.

15. Возможность сканирования файлов во время запуска ОС.

16. Возможность сканирования WMI и системного реестра, всех разделов и подразделов, что обеспечивает защиту от вредоносного программного кода и злонамеренных ссылок, которые распространяются в виде данных.

17. Наличие встроенного инструмента, что объединяет несколько утилит для очистки остатков сложных устойчивых угроз, таких как Conficker, Sirefef, Necurs и другие.

18. Сканирование компьютера в неактивном состоянии.

19. Возможность определения подробных параметров работы антивирусного сканера, таких как определение объектов и методов сканирования, возможность установки максимального размера и времени сканирования файла, максимальная глубина вложения архива и создание исключений.

20. Использование не менее 64-битного ядра для сканирования, что уменьшает нагрузку на систему и позволяет сделать самые быстрые и эффективные сканирования.

21. Возможность использования технологий машинного обучения для более углубленного анализа кода с целью выявления вредоносного поведения и характеристик вредоносного программного обеспечения.

22. Модуль защиты от эксплойтов, который обеспечивает защиту от угроз, способных использовать уязвимости различных приложений, таких как Java, Flash и других.

23. Наличие модуля, способного глубоко анализировать запущенные процессы и их деятельность в файловой системе, обеспечивающего дополнительный уровень защиты от программ-вымогателей (ransomware).

24. Наличия модуля сканирования оперативной памяти, способного отслеживать работу подозрительно запущенных процессов, что позволяет предотвратить заражение даже тщательно зашифрованных и скрытых угроз.

25. Наличие системы обнаружения вторжений (HIPS), которая отслеживает запуск программ и изменения в системном реестре и защищает компьютер от вредоносных программ и нежелательной активности.

26. Возможность создавать собственные правила для контроля запущенных процессов, исполняемых файлов и разделов реестра.

27. Наличие функции дополнительной проверки запущенных процессов в облачном репутационном сервисе.

28. Возможность интеграции защиты рабочих станций и серверов с облачной песочницей (при наличии дополнительной лицензии) без необходимости установки дополнительных программных продуктов.

29. Наличие функции автоматической антивирусной проверки сменных носителей информации.

30. Наличие инструмента, который сможет осуществлять контроль подключения, к рабочей станции сменных носителей информации путем создания правил доступа, а именно блокировка, разрешение, только чтение, чтение и запись, предупреждение.

31. Возможность осуществлять контроль подключения к рабочей станции внешних устройств по типу, по производителю, модели или серийному номеру устройства.

32. Возможность создавать группы разрешенных или запрещенных внешних устройств.

33. Возможность запрещать или разрешать подключение внешних устройств как для всех, так и для отдельных пользователей или групп Windows или домена.

34. Возможность задавать временные интервалы, позволяющего более гибко настраивать правила контроля устройств.

35. Программный продукт должен обеспечивать дополнительный уровень защиты почтового трафика на рабочей станции путем интеграции в почтовый клиент с возможностью проверки POP3, POP3S, SMTP, IMAP и IMAPS и проверки почтовых вложений, особенно на конечных устройствах, которые временно или постоянно находятся за пределами корпоративной сети.

36. Иметь возможность автоматически удалять или перемещать зараженную почту в указанный каталог в почтовом клиенте.

37. Наличие модуля защиты от спама, собственной разработки, с возможностью интеграции в почтовый клиент, что обеспечивает дополнительный уровень защиты от спама, особенно на конечных устройствах, которые временно или постоянно находятся за пределами корпоративной сети.

38. Возможность использовать белые и черные списки спам-адресатов как пользовательские (гибкая персонализация интеллектуального спам-модуля), так и глобальные, информация, которая приходит с серверов обновления.

39. Наличие возможности обеспечить дополнительный уровень защиты Интернет-трафика путем проверки HTTP, HTTPS трафика, что позволит не только блокировать файлы, которые передаются этими протоколами, но и блокировать адреса таких опасных ресурсов, как фишинговые сайты, серверы ботнетов, командные (C&C) серверы APT, а также серверы, которые распространяют угрозы класса «ransomware».

40. Возможность создания списков заблокированных, разрешенных или исключенных из проверки URL-адресов.

41. Возможность блокировать загрузку из Интернета файлов по указанному расширению, особенно на конечных устройствах, которые временно или постоянно находятся за пределами корпоративной сети.

42. Возможность проверки протокола SSL как в автоматическом, так и в интерактивном режимах.

43. Возможность проверки действительности и целостности сертификатов SSL-трафика.

44. Возможность управлять списками доверенных сертификатов и сертификатов, исключенных из проверки, а также возможность выбора действия при определении сертификата недействительным, неопределенным или поврежденным.

45. Наличие дополнительного модуля, который позволяет запускать браузеры в защищенном режиме с целью блокирования попыток вмешательства в область памяти браузера и содержимого его окон, а также дополнительной защиты критических Интернет-соединений, таких как Интернет-платежи и Интернет-банкинг и т.д.

46. Возможность создания исключений по проверке трафика для отдельных программ и отдельных IP-объектов (IP-адресов, диапазонов IP-адресов, подсетей).

47. Наличие персонального брандмауэра для осуществления сетевой фильтрации и защиты как от внешних, так и от локальных сетевых атак.

48. Наличие в персональном брандмауэре интерактивного режима, что предоставляет подробную информацию о новом неизвестном сетевом соединении и дает возможность не только создавать на ПК новое правило сетевой фильтрации для обнаруженного соединения, но и указывать подробные настройки для него.

49. Наличие в персональном брандмауэре режима обучения, что позволяет администратору удаленно настраивать разрешительные правила для сетевых приложений и оборудования.

50. Наличие редактора правил, что позволяет не только редактировать вновь созданные правила, но и управлять встроенными правилами, которых достаточно для первичной тщательной защиты от несанкционированных сетевых соединений и локальных сетевых атак.

51. Возможность создания правил сетевой фильтрации для конкретных программ и сервисов.

52. Возможность создания для персонального брандмауэра различных профилей, которые могут автоматически переключаться, в зависимости от того, к какой сети подключен компьютер.

53. Возможность использовать в персональном брандмауэре дополнительную аутентификацию сети с целью предотвращения несанкционированного подключения ПК к неизвестным опасным сетям.

54. Наличие дополнительного функционала персонального брандмауэра, позволяющего просматривать всю подробную информацию по всем имеющимся сетевым соединениям, а также предупреждать пользователя о подключении к незащищенной сети Wi-Fi.

55. Возможность настройки дополнительных параметров модуля системы обнаружения вторжений (IDS) с целью выявления различных типов возможных сетевых атак на компьютер.

56. Наличие технологии, которая обеспечит защиту от угроз типа «ботнет».

57. Защита уязвимостей сетевого протокола, что улучшает выявление угроз, которые используют недостатки сетевых протоколов, таких как SMB, RPC, RDP и других

58. Наличие внедренных методов выявления различных атак, которые пытаются использовать уязвимости программного обеспечения и предоставить более подробную информацию об идентификаторах CVE.

59. Наличие дополнительного функционала персонального брандмауэра, что дает возможность просматривать на ПК перечень заблокированных IP-адресов, предоставлять информацию о причинах попадания в черный список и позволяет сделать исключения для конкретных безопасных сетевых адресов.

60. Наличие дополнительного функционала персонального брандмауэра, который способен обнаруживать те изменения в сетевых программах, которые повлекли за собой новые несанкционированные сетевые соединения.

61. Возможность фильтрации различного Интернет-трафика.

62. Наличие модуля веб-контроля, позволяющего ограничивать доступ к определенным категориям сайтов.

63. Наличие 27 категорий фильтрации Интернет-трафика, в которых распределены более 100 подкатегорий, а также возможность самостоятельно создавать группы по категориям и подкатегориям.

64. Возможность создавать правила фильтрации Интернет-трафика для разных пользователей и групп ОС Windows или домена.

65. Возможность задавать временные интервалы, что позволяет более гибко настраивать правила веб-фильтрации.

66. Наличие возможности проводить регламентное обновление вирусных баз не менее 24 раз в сутки.

67. Возможность получать обновления клиентов из локального хранилища на сервере, что позволяет поддерживать актуальность антивирусной защиты в закрытых, изолированных сетях, у которых нет доступа к сети Интернет.

68. Возможность создания зеркала обновлений на основе решений производителя для защиты конечных точек.

69. Возможность получения обновлений базы вирусных сигнатур из резервных источников, если основной источник обновления будет недоступен.

70. Возможность для портативных компьютеров получать обновления с серверов производителя онлайн, в случае нахождения за пределами корпоративной сети.

71. Наличие функции позволяющей откатить обновления с возможностью вернуться к предыдущим версиям баз вирусных сигнатур и модулей обновления, и возможностью временно приостановить обновления или устанавливать новые вручную.

72. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.

73. Наличие инструментов мониторинга, оценки состояния безопасности и реагирования.

74. Наличие механизма контроля за состоянием безопасности и актуальностью обновлений ОС.

75. Наличие инструмента для диагностики состояния системы, который может создавать снимки состояния операционной системы для дальнейшего глубоко анализа различных аспектов работы операционной системы, включая запущенные процессы, контент реестра, установленное ПО, сетевые соединения.

76. Возможность определения уровня критичности (опасный, неизвестный, малоизвестный, безопасный) значений различных параметров операционной системы с целью выявления несанкционированных и опасных изменений в операционной системе.

77. Возможность сравнивать различные снимки состояния системы с целью обнаружения изменений, которые произошли в системе за определенное время.

78. Возможность создавать и удаленно выполнять скрипты, что позволит на удаленном ПК останавливать запущенные процессы и службы, удалять ветки реестра, блокировать сетевые соединения.

79. Возможность локального хранения журналов на рабочих станциях.

80. Наличие планировщика задач, который позволит создавать запланированные задачи, среди которых запуск внешней программы, проверка файлов при запуске системы, создание снимка состояния системы, проверка компьютера, обновление вирусных баз и модулей программы.

81. Возможность планирования задач, которые будут запускаться однократно, периодически, а также при условии возникновения конкретных событий.

82. Возможность создания в планировщике нескольких однотипных задач с разной периодичностью или разными условиями запуска.

83. Возможность создания загрузочного диска как на CD-, так и USB-носителях с установленным антивирусным продуктом.

84. Возможность защиты паролем параметров решения для защиты конечной точки.

85. Наличие режима переопределения политики, что дает системному администратору временную возможность изменять на ПК те настройки антивирусного продукта, которые назначаются политикой и недостижимые для редактирования, с целью гибкой настройки антивирусного ПО в специфической среде.

86. Наличие графического интерфейса, совместимого с сенсорным экраном высокого разрешения.

87. Возможность гибко настраивать уведомления и сообщения о событиях на рабочем столе пользователя.

88. Возможность удаленной установки на клиентскую рабочую станцию.

89. Возможность предустановки на отдельных ПК или в образе VDI с помощью комплексного инсталлятора, что позволит соединяться с сервером управления сразу после подключения к сети или запуска в среде VDI.

90. Возможность разрешить обновление компонентов в автоматическом режиме, что позволяет загрузить и установить компоненты без вмешательства администратора или пользователя.

91. Возможность обновления компонентов в ручном режиме, что позволяет обновлять компоненты на неуправляемых рабочих станциях.

92. Возможность обновления некоторых компонентов без необходимости перезагрузки для начала функционирования.

93. Поддержка работы программ, которые работают в полноэкранном режиме, с возможностью скрыть все сообщения от антивирусного ПО.

94. Возможность, кроме основного, указать резервные сервера администрирования.

95. Наличие инструмента удаленного управления.

96. Фактическое низкое потребление ресурсов ПК актуальным антивирусным продуктом (совместно с всеми процессами: графический интерфейс, процесс комплексной защиты, служба удаленного администрирования): не менее 50-100 МБ оперативной памяти, 2-35% центрального процессора.

97. Поддержка ОС: Microsoft Windows /10/11; Ubuntu Desktop 20.04 LTS не менее 64-bit / 22.04 LTS не менее 64-bit / 24.04 LTS не менее 64-bit; Red Hat Enterprise Linux не менее 8/9/10; Linux Mint не менее 21/22; Debian не менее 12/13; MacOS не менее 11/12/13/14/15/26.

Защита серверов

1. Возможность автоматического определения ролей сервера для создания автоматических исключений для специфических файлов, папок, приложений, позволяющее минимизировать влияние на работу серверной операционной системы.

2. Программное обеспечение должно предоставлять защиту от вредоносных программ, троянского ПО, клавиатурных шпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциального нежелательного и опасного ПО.

3. Наличие функции обеспечения защиты в режиме реального времени.

4. Программное обеспечение, во время сканирования, должно использовать эвристические технологии.

5. Возможность проводить антивирусное сканирование по требованию пользователя или администратора и согласно графику.

6. Предоставлять возможность сканирования Hyper-V на наличие вирусов, позволяющее сканировать диски сервера Microsoft Hyper-V Server, то есть виртуальные машины (ВМ), без необходимости установки каких-либо агентов на соответствующих виртуальных машинах.

7. Наличие модуля защиты документов Microsoft Office, позволяющий проверять макросы на наличие вредоносного кода.

8. Обеспечение защиты от эксплойтов, которая обеспечивает защиту от угроз, способных использовать уязвимости Java, Flash и других приложений.

9. Наличие дополнительного уровня защиты пользователей от программ-вымогателей контролирует и оценивает все программы на основе их поведения и репутации.

10. Возможность интеграции защиты рабочих станций и серверов с облачной песочницей (при наличии дополнительной лицензии) без необходимости установки дополнительных программных продуктов.

11. Наличие возможности сканирования интерфейса UEFI с целью проверка на наличие вредоносного программного обеспечения в главной загрузочной записи.

12. Возможность сканирования файлов во время запуска операционной системы.

13. Наличие расширенного сканера памяти, сканирующего и отслеживающего подозрительные процессы, как только они возникают, что позволяет предотвратить заражение даже тщательно зашифрованных и скрытых угроз.

14. Наличие функции сканирования компьютера в неактивном состоянии.

15. Возможность определения подробных параметров работы антивирусного сканера, таких как определение объектов и методов сканирования, возможность установки максимального размера и времени сканирования файла, максимальная глубина вложения архива и создание исключений.

16. Наличие функции автоматической антивирусной проверки сменных носителей информации.

17. Возможность контролировать сменные носители информации с возможностью создания правил (политик) по типу устройства, действиям, изготовителю, модели и серийному номеру устройства.

18. Наличие инструмента, который сможет осуществлять контроль подключения к рабочей станции периферийных устройств путем создания правил доступа по типу устройства, по уровню доступа, по производителю, модели или серийному номеру устройства. Правила (политики) должны иметь возможность быть созданы как для всех, так и для отдельных пользователей или групп пользователей Windows.

19. Наличие системы обнаружения вторжений (HIPS), защищающей компьютер от вредоносных программ и нежелательной активности. Также этот модуль должен содержать мастер для создания правил и редактор правил для контроля запущенных процессов, используемых файлов и разделов реестра.

20. Возможность проводить дополнительную проверка запущенных процессов в облачном репутационном сервисе.

21. Возможность обеспечить защиту почтового клиента на рабочей станции с возможностью интеграции в почтовый клиент, проверка POP3, POP3S, SMTP, IMAP и IMAPS и обеспечение проверки почтовых вложений.

22. Иметь возможность автоматически удалять или перемещать зараженную почту в указанный каталог в почтовом клиенте.

23. Наличие инструмента проверки HTTP, HTTPS трафика с возможностью создания писем, исключенных из проверки, заблокированных и разрешенных URL.

24. Возможность блокировать загрузку из Интернета файлов по указанному расширению.

25. Возможность проверки протокола SSL и проверки подлинности и целостности сертификатов. Возможность управления списками доверенных сертификатов и сертификатов, исключенных из проверки, а также возможность выбора действия при определении сертификата недействующим, неопределенным или поврежденным.

26. Возможность создания исключений из проверки трафика для отдельных программ и отдельных IP-объектов (IP-адресов, диапазонов IP-адресов, подсетей).

27. Возможность настройки дополнительных параметров модуля системы обнаружения вторжений (IDS) для выявления различных типов возможных сетевых атак на компьютер.

28. Возможность использования технологии, обеспечивающей защиту от угроз типа «ботнет».

29. Защита уязвимостей сетевого протокола, улучшающая обнаружение угроз, использующих недостатки сетевых протоколов, таких как SMB, RPC, RDP и др.

30. Наличие возможности проводить регламентное обновление вирусных баз не менее 24 раз в сутки.

31. Получение обновления для клиентских устройств из локального зеркала на сервере.

32. Возможность создания зеркала обновления средствами антивирусного ПО.

33. Возможность обновления вирусных баз из резервных источников, если основной источник обновления будет недоступным.

34. Наличие функции отката обновлений с возможностью вернуться к предыдущим версиям баз вирусных сигнатур и модулей обновления, и возможностью временно приостановить обновления или устанавливать новые вручную.

35. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.

36. Наличие инструмента удаленного управления.

37. Возможность, помимо основного, указать резервные серверы администрирования.

38. Наличие механизма контроля актуальности обновлений операционной системы.

39. Наличие инструмента для диагностики системы, который может создавать снимки состояния операционной системы для дальнейшего глубоко анализа различных аспектов работы операционной системы, включая запущенные процессы, контент реестра, установленное ПО, сетевые соединения. Благодаря умению сравнивать различные снимки состояния системы, этот инструмент может обнаружить изменения, которые произошли в системе. Также он может создавать и выполнять скрипты, что позволит останавливать запущенные процессы, удалять ветки реестра, блокировать сетевые соединения.

40. Наличие планировщика задач, который позволит создавать запланированные задачи, включая запуск внешней программы, проверку файлов при запуске системы, создание снимка состояния системы, проверку компьютера, обновление вирусных баз и модулей программы.

Возможность планировать задачи, которые будут запускаться однократно, периодически и при возникновении конкретных событий.

41. Возможность создания в планировщике нескольких однотипных задач с разной периодичностью или разными условиями запуска.

42. Возможность работы в кластерах как домена, так и рабочей группы.

43. Возможность настройки быстродействия, указывая количество потоков сканирования.

44. Возможность настройки режима запуска путем отключения графического интерфейса для терминальных пользователей, что позволяет уменьшить нагрузку на сервер, работающий в режиме сервера терминалов.

45. Возможность создания загрузочного диска как на CD-, так и на USB-носителях с установленным антивирусным продуктом.

46. Поддержка работы программ, работающих в полноэкранном режиме, с возможностью скрыть все сообщения от антивирусного ПО.

47. Возможность защиты паролем от изменения параметров и удаления антивирусного ПО.

48. Возможность удаленной установки на сервер.

49. Возможность предустановки на отдельных серверах с помощью комплексного инсталлятора, что позволит соединяться с сервером управления сразу после подключения к сети.

50. Возможность интеграции с облачным сервисом Microsoft Azure.

51. Поддержка ОС: Microsoft Windows Server не менее 2025/2022/2019/2016/2012 R2/2012; Red Hat Enterprise Linux (RHEL) не менее 8/9/10; Rocky Linux -v.8/-v.9/-v.10; Ubuntu Server 22.04 LTS/24.04 LTS; Debian 11/12/13; SUSE Linux Enterprise Server (SLES) 15/16; Alma Linux не менее 8/9/10; Rocky Linux не менее 8/9/10; Oracle Linus не менее 8/9/10; Amazon Linux не менее 2023.

Требования законодательства

1. Предлагаемое программное решение должно соответствовать по надежности и безопасности международным стандартам, стандартам и техническим регламентам, которые относятся к данной отрасли.