«Утверждаю»
Главный метролог
ООО «Бухарский НПЗ»
_____А.Р.Хамроев
«__14__» ___02_____2024г

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на приобретение прав пользования программными средствами антивирусной защиты рабочих станций, серверов, с использованием технологии облачной песочницы для защиты от вредоносного ПО , программ-вымогателей и «0-дневных» угроз.

Каравулбазар 2024.

Общие требования расширенной антивирусной защиты рабочих станций, серверов и мобильных устройств с использованием технологии облачной песочницы от вредоносного ПО , программ-вымогателей и «0-дневных» угроз

Антивирусная защита (АЗ) Protect версии Advanced типа On-Prem должна представлять собой масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети рабочих станций и серверов с использованием технологии облачной песочницы.

В рамках всей организации должны использоваться единые антивирусные средства. Отдельно стоящие персональные компьютеры, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус).

Технические параметры программных средств антивирусной защиты должны соответствовать или превосходить следующие указанные параметры:

Сервер управления

1. Возможность централизованного управления антивирусной защитой всей сетевой Инфраструктуры через консоль Protect.
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 рабочих станциях 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. Удаленная установка антивирусного программного обеспечения для операционных систем Windows, Linux и Mac на несколько конечных точек одновременно.
6. Удаленная установка пользовательского программного обеспечения.
7. Возможность удаленного удаления установленного пользовательского программного обеспечения.
8. Удаленное удаление антивирусного программного обеспечения для операционных систем Windows, Linux и Mac.
9. 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.
10. Наличие инструмента для создания и редактирования установочных пакетов для операционных систем Windows, Linux и Mac 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.
11. Наличие диспетчера пользователей, который позволяет создавать разных 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.
12. Возможность аутентифицировать администраторов консоли управления с помощью групп безопасности Active Directory.
13. Возможность использования двухфакторной аутентификации для учетных записей администраторов, что позволяет предотвратить несанкционированное подключение к серверу централизованного управления.
14. Наличие журнала аудита, в котором регистрируются и отслеживаются все изменения в конфигурации и все действия, которые выполняют пользователи сервера администрирования.
15. 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.
16. Возможность создавать и редактировать статические группы и возможность импорта из Active Directory дерева компьютеров.
17. Возможность настройки автоматического распределения клиентов по динамическим группам по многим критериям с последующим назначением соответствующих политик безопасности, а также запуском необходимых задач.
18. Возможность импорта пользователей и групп из Active Directory для дальнейшего использования их для персонализации правил контроля устройств и веб-контроля.
19. Возможность использовать как встроенные, так и пользовательские политики, предназначенные для постоянного обслуживания конфигурационных настроек антивирусных продуктов. Возможность осуществлять экспорт/импорт политик.
20. Наличие панели мониторинга, которая предоставляет всю необходимую подробную информацию относительно уровня защиты безопасности инфраструктуры, состояния защищенных конечных точек, а также состояния самого сервера администрирования.
21. Наличие около 100 предустановленных шаблонов отчетов, которые могут использоваться как для панели мониторинга, так и для формирования различных отчетов.
22. 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.
23. Поддержка инструментом удаленного администрирования следующих баз данных: MS SQL Server, MySQL.
24. Возможность экспортировать журналы в syslog для дальнейшей интеграции с SIEM.
25. Возможность настраивать параметры журналов и отчетов или выбрать из более чем 50 шаблонов для различных систем/клиентов.
26. Возможность создавать зеркало обновлений с помощью антивирусного продукта, специальной утилиты или прокси сервера.
27. Возможность создания зеркала обновлений на основе сторонних HTTP-серверов.
28. Веб-ориентированный интерфейс, который дает возможность управлять сервером через любой браузер путем соединения, защищенного сертификатом.
29. 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.
30. Возможность отслеживать установленное на рабочей станции ПО, а также удалять установленное ПО на выбор.

31. Дополнительный компонент, что позволяет управлять антивирусной защитой на мобильных устройствах.
32. Специальный компонент, который осуществляет обнаружение в сети незащищенных рабочих станций для дальнейшего развертывания антивирусной защиты.
33. Защита соединений между компонентами сервера с помощью как самостоятельно выпущенных сертификатов, так и существующих сертификатов.
34. Инструмент для управления состоянием лицензий (даже без использования сервера администрирования).
35. Возможность деактивировать лицензию антивирусных продуктов даже на рабочих станциях, к которым нет физического или удаленного доступа.
36. Возможность установки сервера администрирования на ОС Windows и Linux.
37. Поставка сервера администрирования в развернутом виде, готовом для использования в виртуальных средах, таких как Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).
38. Поддержка систем виртуализации, таких как VMware Horizon 8.x или Citrix XenCenter/XenServer 8+.
39. Возможность определять, какая виртуальная машина будет являться источником для копирования или клонирования в системах VDI.
40. Наличие мастера настройки для определения подробных параметров для интеграции с системами VDI.
41. Возможность выбирать варианты обработки идентификаторов клонированных компьютеров, такие как сопоставление существующими компьютерами или создание новых компьютеров.
42. Возможность определять параметры шаблона именования VDI для мгновенных клонов или каталогов машин.
43. Наличие предустановленных шаблонов в системе уведомлений для информирования о некорректной идентификации клонированных машин, что дает возможность оповещать о некорректно настроенной интеграции с системами VDI.
44. Наличие автоматического обновления агента управления, что дает возможность без вмешательства администраторов использовать актуальные версии.
45. Наличие механизма распределения автоматического процесса обновления, что дает возможность снизить нагрузку на сеть и компьютеры в целом.
46. Возможность установки агента управления на ARM64 процессорах.
47. Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам.
48. Наличие функционала для определения администратора площадки или филиала с соответствующей частью лицензии.

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. Антивирусное сканирование по требованию пользователя или администратора и в соответствии с графиком.
14. Модуль защиты документов, которые дают 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 других
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 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. Модуль, который глубоко анализирует запущенные процессы и их деятельность в файловой системе, что обеспечивает дополнительный уровень защиты от программ вымогателей (ransomware).
24. Модуль сканирования оперативной памяти, который способный отслеживать работу подозрительных запущенных процессов, что позволяет предотвратить заражение

даже тщательно зашифрованными и скрытыми угрозами.
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. Дополнительная проверка 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. Автоматическая антивирусная проверка сменных носителей.
30. Наличие инструмента, который сможет осуществлять контроль подключения к рабочей станции сменных носителей 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 устройства, 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, что позволяет более гибко настраивать правила контроля устройств.
35. Обеспечение дополнительного уровня 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 тех ПК, которые временно или постоянно находятся за пределами корпоративной сети.
36. 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 тех ПК, 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 к которым приходит с серверов обновления.
39. Обеспечение дополнительного уровня защиты Интернет-трафика путем проверки HTTP, HTTPS трафика, что позволяет 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 тех ПК, которые временно или постоянно находятся за пределами корпоративной сети.
42. Возможность проверки протокола SSL как в автоматическом, так и в интерактивном режимах.
43. Проверка 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 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, что позволяет 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. Возможность использования технологии, которая обеспечивает 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. Возможность просматривать на ПК автоматически заблокированные сетевые соединения и при необходимости временно разрешать конкретные безопасные сетевые соединения.
60. Наличие дополнительного функционала персонального брандмауэра, что дает возможность просматривать на ПК перечень заблокированных IP-адресов, предоставляет информацию о причинах попадания в черный список и позволяет сделать исключения для конкретных безопасных адресов.
61. Наличие дополнительного функционала персонального брандмауэра, который способен обнаруживать те изменения в сетевых программах, которые повлекли за собой новые несанкционированные сетевые соединения.

62. Фильтрация Интернет-трафика.
63. Наличие модуля веб-контроля, что позволяет ограничивать доступ к определенным категориям сайтов.
64. 27 категорий фильтрации Интернет-трафика, в которых распределены более 100 подкатегорий, а также возможность создавать группы по категориям и подкатегориям.
65. Возможность создавать правила фильтрации Интернет-трафика для разных пользователей и групп ОС Windows или домена.
66. Возможность задавать временные интервалы, что позволяет более гибко настраивать правила веб-фильтрации.
67. Регламентное обновление вирусных баз не менее 24 раз в сутки.
68. Получение обновления клиентов из локального хранилища на сервере, что позволяет поддерживать актуальность антивирусной защиты в закрытых изолированных сетях, у которых нет доступа к сети Интернет.
69. Возможность создания зеркала обновлений на основе решений для защиты конечных точек.
70. Возможность получения обновлений вирусных баз из резервных источников, если основной источник обновления будет недостижим.
71. Возможность для портативных компьютеров получать обновления с серверов производителя онлайн, в случае нахождения за пределами корпоративной сети.
72. Откат обновлений с возможностью вернуться к предыдущим версиям баз вирусных сигнатур и модулей обновления и возможностью временно приостановить обновления или устанавливать новые вручную.
73. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.
74. Инструменты мониторинга, оценки состояния безопасности и реагирование:
75. Наличие механизма контроля за состоянием безопасности и актуальностью обновлений ОС.
76. 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.
77. Возможность определения уровня критичности (опасный, неизвестный, малоизвестный, безопасный) значений различных параметров операционной системы с целью выявления несанкционированных и опасных изменений в операционной системе.
78. Возможность сравнивать различные снимки состояния системы с целью обнаружения изменений, которые произошли в системе за определенное время.
79. Возможность создавать и удаленно выполнять скрипты, что позволит на удаленном ПК останавливать запущенные процессы и службы, удалять ветки реестра, блокировать сетевые соединения.
80. Локальное хранение журналов на рабочих станциях.
81. 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.
82. Возможность планирования задач, которые будут запускаться однократно, периодически, а также при условии возникновения конкретных событий.
83. Возможность создания в планировщике нескольких однотипных задач с разной периодичностью или разными условиями запуска.
84. Возможность создания загрузочного диска как на CD-, так и USB-носителях с установленным антивирусным продуктом.

85. Возможность защиты паролем параметров решения для защиты конечной точки.
86. Наличие режима переопределения политики, что дает системному администратору временную возможность изменять на ПК те настройки антивирусного ПО, которые назначаются политикой и недостижимые для редактирования, с целью гибкой настройки антивирусного ПО в специфической среде.
87. Графический интерфейс, совместимый с сенсорным экраном высокого разрешения.
88. Возможность гибко настраивать уведомления и сообщения о событиях на рабочем столе пользователя.
89. Возможность удаленной установки на клиентскую рабочую станцию.
90. 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.
91. Возможность разрешить обновление компонентов в автоматическом режиме, что позволяет загрузить и установить компоненты без вмешательства администратора или пользователя.
92. Возможность обновления компонентов в ручном режиме, что позволяет обновлять компоненты на неуправляемых рабочих станциях.
93. Возможность обновления некоторых компонентов без необходимости перезагрузки для начала функционирования.
94. Поддержка работы программ, которые работают в полноэкранном режиме, с возможностью скрыть все сообщения от антивирусного ПО.
95. "В антивирусном продукте должны использоваться не заимствованные, а собственные технологические разработки для эффективной работы всех основных модулей и сервисов. Например:
- ядро обнаружения, что содержит множество актуальных методов обнаружения,
- облачный репутационный сервис и система своевременного обнаружения,
- технология, что уменьшает время сканирования и нагрузки на ОС,
- интеллектуальное ядро антиспама,
- технология для уменьшения использования ресурсов виртуальной среды."
96. Возможность, кроме основного, указать резервные сервера администрирования.
97. Наличие инструмента удаленного управления.
98. Низкое потребление ресурсов ПК актуальными антивирусными продуктами (совместно с всеми процессами: графический интерфейс, процесс комплексной защиты, служба удаленного администрирования): 50-100 МБ оперативной памяти, 2-35 % центрального процессора.
99. Наличие многоязычного инсталлятора, который включает в себя в том числе русский язык.
100.Поддержка ОС: Microsoft Windows 7 (SP1); Microsoft Windows 8; Microsoft Windows 8.1; Microsoft Windows 10; Microsoft Windows 11; Ubuntu Desktop 18.04 LTS 64-bit; Ubuntu Desktop 20.04 LTS; Ubuntu Desktop 22.04 LTS; Red Hat Enterprise Linux 7, 8 .; SUSE Linux Enterprise Desktop 15; Linux Mint 20; macOS 10.12 или выше; Android 5 (Lollipop) или выше;

Защита серверов

1. Автоматическое определение ролей сервера для создания автоматических исключений для специфических файлов, папок, приложений, позволяющее минимизировать влияние на работу серверной операционной системы.
2. Предоставление защиты от вредоносных программ, троянского ПО, клавиатурных шпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциального нежелательного и опасного ПО.
3. Обеспечение защиты в режиме реального времени.

4. Использование эвристических технологий во время сканирования.
5. Антивирусное сканирование по требованию пользователя или администратора и согласно графику.
6. Сканирование 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. Модуль защиты документов Microsoft Office, позволяющий проверять макросы на наличие вредоносного кода.
8. Защита от эксплойтов, которая обеспечивает защиту от угроз, способных использовать уязвимости Java, Flash и других приложений.
9. Дополнительный уровень 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. Сканирование интерфейса UEFI – проверка на наличие вредоносного программного обеспечения в главной загрузочной записи.
12. Возможность сканирования файлов во время запуска операционной системы.
13. Расширенный сканер памяти отслеживает и сканирует подозрительные процессы, как только они возникают, что позволяет предотвратить заражение даже тщательно зашифрованными и скрытыми угрозами.
14. Сканирование 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. Автоматическая антивирусная проверка сменных носителей.
17. Контроль сменных носителей с возможностью создания правил 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 могут быть созданы как для всех, так и для отдельных пользователей или групп Windows.
19. Наличие системы обнаружения вторжений (HIPS), защищающей компьютер от вредоносных программ и нежелательной активности. Также этот модуль содержит мастер для создания правил и редактор правил для контроля запущенных процессов, используемых файлов и разделов реестра.
20. Дополнительная проверка запущенных процессов в облачном репутационном сервисе.
21. Обеспечение защиты почтового клиента на рабочей станции с возможностью интеграции в почтовый клиент, проверка POP3, POP3S, SMTP, IMAP и IMAPS и обеспечение проверки почтовых вложений.
22. Возможность автоматически удалять или перемещать зараженную почту в указанный каталог в почтовом клиенте.
23. Проверка 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 других
30. Регламентное обновление вирусных баз не менее 24 раз в сутки.
31. Получение обновления клиентов 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. Откат 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 планирования задач, 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 файловый сервер.
49. Возможность предустановки на отдельных файловых серверах с помощью комплексного инсталлятора, что позволит соединяться с сервером управления сразу после подключения к сети.
50. Поддержка ОС: Microsoft Windows Server 2008, 2008R2, 2012R2, 2012, 2016, 2019, 2022; RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, RedHat Enterprise Linux (RHEL) 9, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Ubuntu Server 22.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12,SUSE Linux Enterprise Server (SLES) 15,Oracle Linux 8, Amazon Linux 2

Решение для полнодискового шифрования

1. Управления полным шифрованием диска на управляемых рабочих станциях Windows и MacOS с дополнительным уровнем защиты на этапе предзагрузочного входа.
2. Наличие инструмента удаленного управления.
3. Возможность удаленной установки на клиентскую рабочую станцию.
4. Возможность предустановки на отдельных ПК с помощью комплексного инсталлятора, что позволит соединяться с сервером управления сразу после подключения к сети.
5. Возможность удаленного полнодискового шифрования/расшифровки всех дисков.
6. Возможность удаленного полнодискового шифрования/расшифровки только загрузочного диска.
7. Возможность использовать для шифрования дополнительные технологии от производителей оборудования: такие как доверенный платформенный модуль (TPM) или самошифрованные диски (OPAL).
8. Наличие в консоли сервера управления мастера включения шифрования, что позволяет администратору очень удобно и быстро выбрать для удаленной рабочей станции соответствующую политику с необходимыми параметрами и запустить на ней процесс шифрования дисков.
9. Возможность для пользователей каждой рабочей станции создавать свой собственный пароль предзагрузочного входа.
10. Возможность администратору устанавливать для предзагрузочного пароля различные критерии, такие как: сложность пароля, количество попыток ввода, срок действия.
11. Различные режимы для графического пользовательского интерфейса: обычный, где будет доступен весь функционал графического интерфейса или минимальный, когда будут отображаться только уведомления.
12. Поддержка работы программ, работающих в полноэкранном режиме, с возможностью скрыть все сообщения, связанные с шифрованием.
13. Возможность пользователя изменить свой загрузочный пароль с помощью текущего пароля
14. Возможность для администратора создавать пароль восстановления в случае, если пользователь забыл свой собственный пароль.
15. Возможность для администратора создавать загрузочный диск или USB-накопитель для аварийной расшифровки диска в случае, если к данным на зашифрованном диске нельзя будет получить доступ с помощью стандартных средств.
16. Возможность для администратора удаленно аннулировать предзагрузочный пароль, что приведет к отображению пользователю запроса на изменение пароля и заставит его изменить пароль при последующей перезагрузке ОС.

17. Возможность для администратора удаленно блокировать предзагрузочный пароль, что приведет к отключению предзагрузочного входа после последующей перезагрузки, а для разблокировки необходимо будет установить новый предзагрузочный пароль с помощью пароля восстановления.
18. Возможность для администратора удаленно стереть предзагрузочный пароль, что приведет к немедленной блокировке удаленной рабочей станции, а пользователю будет отображено на экране сообщение о критической ошибке типа «синий экран». После этого доступ к информации на дисках можно получить только после расшифровки с помощью загрузочного диска восстановления.

Облачная песочница

1. Возможность отправлять подозрительные файлы с рабочих станций и серверов на анализ в облако
2. Возможность отправлять подозрительные вложения писем с почтового сервера на анализ в облако
3. Использование технологий машинного обучения при первичном анализе отправленных файлов
4. Возможность осуществлять непрерывное наблюдение за активностью отправленных файлов (30 дней по умолчанию), что позволяет обнаруживать даже те угрозы, которые способны обходить классическую песочницу.
5. Возможность автоматической блокировки файлов, вызвавших вредоносную активность во время первичного анализа или во время длительного наблюдения в облаке.
6. Возможность обеспечить быструю реакцию по результатам первичного анализа путем блокирования 0-дневных угроз (от нескольких секунд до 10 минут)
7. Наличие системы отчетности, которая предоставляет отчеты о результатах исследования отправленных в облака образцов
8. Возможность осуществлять гибкие настройки отправки подозрительных файлов и определение реакции после первичного анализа или обнаружения вредоносной активности во время длительного наблюдения в облаке.

Необходимая документация для заказчика:

передоставить Авторизационное письмо (MAF) отпроизводителя на имя заказчика а также партнерский сертификат с производителем.

Согласовано:
Начальник IT-центр Фазилов А.А.

Составил:
Начальник сектор Кибербезопасность Бахронов Б.Х.