«Утверждаю»
Главный метролог
ООО «Бухарский НПЗ»
_____А.Р.Хамроев
«_20_» _02_____2023г

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

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

Караулбазар 2023.

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) 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

- Возможность централизованного управления антивирусной защитой всей сетевой инфраструктуры локально, а также управление лицензиями через платформу Business Account.
- 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.
- 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.
- 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.
- 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.
- Поддержка инструментом удаленного администрирования следующих баз данных: MS SQL Server, MySQL.
- Возможность создания зеркала обновлений на основе сторонних HTTP-серверов.
- Возможность настраивать параметры журналов и отчетов или выбрать из более чем 50 шаблонов для различных систем/клиентов.
- Возможность отслеживать установленное на рабочей станции ПО, а также удалять установленное ПО на выбор.
- Возможность деактивировать лицензию антивирусных продуктов даже на рабочих станциях, к которым нет физического или удаленного доступа.

- Наличие функционала для определения администратора площадки или филиала с соответствующей частью лицензии.
- Наличие предустановленных шаблонов в системе уведомлений для информирования о некорректной идентификации клонированных машин, что дает возможность оповещать о некорректно настроенной интеграции с системами VDI.
- Возможность определять, какая виртуальная машина будет являться источником для копирования или клонирования в системах VDI.
- Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам.
- Возможность удаленного полнодискового шифрования/расшифровки всех дисков на клиентских машинах.
- Возможность удаленного полнодискового шифрования/расшифровки только загрузочного диска на клиентских машинах.
- 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.
- Возможность для пользователей каждой рабочей станции создавать свой собственный пароль предзагрузочного входа.
- Возможность администратора устанавливать для предзагрузочного пароля различные критерии, такие как: сложность пароля, количество попыток ввода, срок действия.
- Возможность 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.
- Возможность 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.

Защита рабочих станций

- 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.
- 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.

- 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.
- Возможность делать исключения из сканирования определенных файлов, которые не вредоносные, но сканирование которых может привести к отклонениям в работе или влиять на продуктивность системы.
- Обеспечение антивирусной защиты в режиме реального времени.
- Антивирусное сканирование по требованию пользователя или администратора и в соответствии с графиком.
- Возможность использования технологий машинного обучения для более углубленного анализа кода с целью выявления вредоносного поведения и характеристик вредоносного программного обеспечения.
- Возможность создавать группы разрешенных или запрещенных внешних устройств.
- Наличие встроенного инструмента, что объединяет несколько утилит для очистки остатков сложных устойчивых угроз, таких как Conficker, Sirefef, Necurs и других
- 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.
- Возможность создавать и удаленно выполнять скрипты, что позволит на удаленном ПК останавливать запущенные процессы и службы, удалять ветки реестра, блокировать сетевые соединения.
- Возможность запрещать или разрешать подключение внешних устройств как для всех, так и для отдельных пользователей или групп Windows или домена.
- 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.
- 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.
- Наличие в персональном брандмауэре режима обучения, что позволяет администратору удаленно настраивать разрешительные правила для сетевых приложений и оборудования.
- Возможность использовать в персональном брандмауэре дополнительную аутентификацию сети с целью предотвращения несанкционированного подключения ПК к неизвестным опасным сетям.
- Наличие дополнительного функционала персонального брандмауэра, который способен обнаруживать те изменения в сетевых программах, которые повлекли за собой новые несанкционированные сетевые соединения.
- 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.

- Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.
- 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.
- 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.
- Сканирование компьютера в неактивном состоянии.
- Использование 64-битного ядра для сканирования, что уменьшает нагрузку на систему и позволяет сделать самые быстрые и эффективные сканирования.
- Возможность определения уровня критичности (опасный, неизвестный, малоизвестный, безопасный) значений различных параметров операционной системы с целью выявления несанкционированных и опасных изменений в операционной системе.
- Поддержка ОС: Microsoft Windows 7 (Professional или выше); Microsoft Windows 8 (Professional или выше); Microsoft Windows 8.1 (Professional или выше); Microsoft Windows 10 (Professional или выше); Microsoft Windows 11; Ubuntu Desktop 18.04 LTS (или выше); Debian 9 64-bit (или выше);
- Обеспечение управления полным шифрованием диска на управляемых рабочих станциях Windows с дополнительным уровнем защиты на этапе предзагрузочного входа.
- Возможность использовать для шифрования дополнительные технологии от производителей оборудования: такие как доверенный платформенный модуль (TPM) или самошифрованные диски (OPAL).
- Различные режимы для графического пользовательского интерфейса: обычный, где будет доступен весь функционал графического интерфейса или минимальный, когда будут отображаться только уведомления.
- Поддержка работы программ, работающих в полноэкранном режиме, с возможностью скрыть все сообщения, связанные с шифрованием.
- Возможность пользователя изменить свой предзагрузочный пароль с помощью текущего пароля
- Возможность администратора создавать пароль восстановления в случае, если пользователь забыл свой собственный пароль.
- Возможность 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.
- Возможность администратора удаленно аннулировать предзагрузочный пароль, что приведет к отображению пользователю запроса на изменение пароля и заставит его изменить пароль при последующей перезагрузке ОС.

Защита серверов

- Автоматическое определение ролей сервера для создания автоматических исключений для специфических файлов, папок, приложений, позволяющее минимизировать влияние на работу серверной операционной системы.
- Возможность интеграции защиты рабочих станций и серверов с облачной песочницей (при наличии дополнительной лицензии) без необходимости установки дополнительных программных продуктов.
- Сканирование интерфейса UEFI – проверка на наличие вредоносного программного обеспечения в главной загрузочной записи.
- Использование эвристических технологий во время сканирования.
- Предоставление защиты от вредоносных программ, троянского ПО, клавиатурных шпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциального нежелательного и опасного ПО.
- Регламентное обновление вирусных баз не менее 24 раз в сутки.
- Возможность помимо основного указать резервные серверы администрирования.
- 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.
- 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.
- Возможность блокировать загрузку из Интернета файлов по указанному расширению.
- Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.
- Наличие специальной технологии, значительно снижающей нагрузку на виртуальные рабочие станции, а также на гипервизор в целом.
- Возможность настройки режима запуска путем отключения графического интерфейса для терминальных пользователей, что позволяет уменьшить нагрузку на сервер, работающий в режиме сервера терминалов.

Облачная песочница

- Возможность отправлять подозрительные файлы с рабочих станций и серверов на анализ в облако.
- Использование технологий машинного обучения при первичном анализе отправленных файлов.

- Возможность осуществлять непрерывное наблюдение за активностью отправленных файлов (30 дней по умолчанию), что позволяет обнаруживать даже угрозы, которые способны обходить классическую песочницу.
- Возможность автоматической блокировки файлов, вызвавших вредоносную активность во время первичного анализа или во время длительного наблюдения в облаке.
- Возможность обеспечить быструю реакцию по результатам первичного анализа путем блокирования 0-дневных угроз (от нескольких секунд до 10 минут).
- Наличие системы отчетности, которая предоставляет отчеты о результате исследования отправленных в облака образцов.
- Возможность осуществлять гибкие настройки отправки подозрительных файлов и определение реакции после первичного анализа или обнаружения злонамеренной активности во время длительного наблюдения в облаке.

Согласовано:

Начальник IT-центр Фазилов А.А.

Составил:

Начальник ИТ сектор Игамбердиев И.И.

Начальник сектор Кибербезопасность Бахронов Б.Х.