Техническая спецификация

по продлению лицензии на программное обеспечение по антивирусной защите рабочих станций и серверов.

Наименование национальных стандартов СТ РК ГОСТ Р 51188-2007(ГОСТ Р 51188-98, IDT)

Антивирусная защита (АЗ) должна представляет собой корпоративное решение, обеспечивающее устойчивое функционирование в сети рабочих станций и серверов. В рамках всей организации используются единые антивирусные средства.

Настоящая Техническая спецификация является основополагающим документом, устанавливающим требования к поставляемому программному обеспечению с оказанием сопутствующих услуг по внедрению системы антивирусной защиты. Все компоненты системы имеют полную интеграцию между собой.

1. Общие требования к программному обеспечению по антивирусной защите

1.1. Общее количество защищаемых узлов: Kaspersky Endpoint Security for Business - Select Kazakhstan Edition. 1 year License **400** рабочих станций и серверов;

1.2. Срок действия лицензии: 12 месяцев с момента генерации лицензий на программное обеспечение.

1.3. Срок поставки: не более 15 календарных дней со дня вступления договора в законную силу.

2.Технические требования к программному обеспечению по антивирусной защите

Антивирусные средства включают:

- программные средства антивирусной защиты для рабочих станций Windows;
- программные средства антивирусной защиты для рабочих станций MacOS;
- программные средства антивирусной защиты для рабочих станций и серверов Linux;
- программные средства антивирусной защиты для файловых серверов Windows;
- программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);
- 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, на русском и английском языке.

Все антивирусные средства, включая средства управления, обладают контекстной справочной системой на русском и английском языке.

Требования к программным средствам антивирусной защиты для рабочих станций Windows

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

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;
- Windows 8 Professional / Enterprise (32 / 64-разрядная);
- Windows 8.1 Professional / Enterprise (32 / 64-разрядная);

- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;
- Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise.

В программном средстве антивирусной защиты 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;
- 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;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- 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;
- возможность установки ограничение длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется.

Требования к программным средствам антивирусной защиты для серверов Windows

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

- 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;
- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

В программном средстве антивирусной защиты 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;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- 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;
- 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.

Требования к программным средствам антивирусной защиты для рабочих станций Mac

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

- macOS 10.14 - 12;

В программном средстве антивирусной защиты 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;
- централизованное управление всеми выпеуказанными компонентами с помощью единой системы управления;
- возможность установки расширений из командной строки с помощью новой команды kav;
- возможность задавать исключения при проверке указанных областей на уровне перехватов файловых операций;
- возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены.

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

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

- CentOS 6.7 и выше.
- Debian GNU/Linux 10.1 и выше.
- Debian GNU/Linux 11.
- Mageia 4.
- Red Hat Enterprise Linux 6.7 и выше.
- Альт 8 СП Рабочая Станция.
- Альт 8 СП Сервер.
- Альт Образование 10.
- Альт Рабочая Станция 10.

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

- AlmaLinux OS 8 и выше.

- AlmaLinux OS 9 и выше.
- AlterOS 7.5 и выше.
- Amazon Linux 2.
- Astra Linux Common Edition 2.12.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
- CentOS 6.7 и выше.
- CentOS 7.2 и выше.
- CentOS Stream 9.
- Debian GNU/Linux 10.1 и выше.
- Debian GNU/Linux 11.
- EMIAS 1.0.
- EulerOS 2.0 SP5.
- LinuxMint 19.2 и выше.
- LinuxMint 20.3 и выше.
- openSUSE Leap 15.0 и выше.
- Oracle Linux 7.3 и выше.
- Oracle Linux 8.0 и выше.
- Red Hat Enterprise Linux 6.7 и выше.
- Red Hat Enterprise Linux 7.2 и выше.
- Red Hat Enterprise Linux 8.0 и выше.
- Red Hat Enterprise Linux 9.
- Rocky Linux 8.5 и выше.
- SUSE Linux Enterprise Server 12.5 и выше.
- SUSE Linux Enterprise Server 15 и выше.
- Ubuntu 20.04 LTS.
- Ubuntu 22.04 LTS.
- Альт 8 СП Рабочая станция.
- Альт 8 СП Сервер.
- Альт Образование 10.
- Альт Рабочая Станция 10.
- Альт Сервер 10.
- Атлант, сборка Alcyone, версия 2022.02.
- Гослинукс 7.17.
- Гослинукс 7.2.
- РЕД ОС 7.3.
- РОСА "Кобальт" 7.9.
- РОСА "Хром" 12.
- ОСОН "ОСНова".

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

- Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
- EulerOS 2.0 SP8.
- SUSE Linux Enterprise Server 15 SP3.
- Ubuntu 20.04 LTS.
- Альт 8 СП Сервер.
- РЕД ОС 7.3.

В программном средстве антивирусной защиты 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;. thz;.tbz2; .gz;.tgz; .arj.;
- проверку сообщений электронной почты в текстовом формате (Plain text);
- 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;
- 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.

Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows

Программные средства антивирусной защиты для файловых серверов Windows функционируют на компьютерах, работающих под управлением операционных систем следующих версий:

32-разрядных операционных систем Microsoft Windows

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше.

64-разрядных операционных систем Microsoft Windows

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Microsoft Small Business Server 2008 Standard / Premium SP2 или выше;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2011 Essentials / Standard SP1 или выше;
- Microsoft Windows MultiPoint Server 2011 Standard / Premium;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
- Microsoft MultiPoint Server 2012 Standard / Premium;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2016 MultiPoint;
- Windows Server 2016 Core Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2016;
- Windows Storage Server 2016;
- Windows Hyper-V Server 2016;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2019 Core;
- Windows Storage Server 2019;
- Windows Hyper-V Server 2019;
- Windows Server 2022;
- Windows 10 Enterprise multi-session.

В программном средстве антивирусной защиты реализованы следующие функциональные возможности:

- антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
- защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
- непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
- анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- проверки контейнеров Microsoft Windows;
- защиты от эксплуатирования уязвимостей в памяти процессов;
- должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
- добавлять процессы в список защищаемых;
- ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
- настройки проверки критических областей сервера в качестве отдельной задачи;
- регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;

- продолжать антивирусное сканирование в фоновом режиме;
- наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
- ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
- интеграции с SIEM системами;
- указания количества рабочих процессов антивируса вручную;
- отключить графический интерфейс;
- наличие удаленной и локальной консоли управления;
- управления параметрами антивируса из командной строки;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
- защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
- включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.

Требования к программным средствам антивирусной защиты мобильных устройств

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

- Android 5.0–13 (включая Android 12L, исключая Go Edition);
- iOS 10–16 или iPadOS 13–15;

В программном средстве антивирусной защиты смартфонов для ОС Android 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.

В программном средстве защиты смартфонов для ОС Apple iOS 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.

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

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

- Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 11 Home 64-разрядная;
- Microsoft Windows 11 Pro 64-разрядная;
- Microsoft Windows 11 Enterprise 64-разрядная;
- Microsoft Windows 11 Education 64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная/64-разрядная;

- Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;
- Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;
- Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Windows Server 2016 Standard (LTSB) 64-разрядная;
- Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
- Windows Server 2019 Standard 64-разрядная;
- Windows Server 2019 Datacenter 64-разрядная;
- Windows Server 2019 Core 64-разрядная;
- Windows Server 2022 Standard 64-разрядная;
- Windows Server 2022 Datacenter 64-разрядная;
- Windows Server 2022 Core 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Storage Server 2016 64-разрядная;
- Windows Storage Server 2019 64-разрядная.

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

- VMware vSphere 6.7;
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Microsoft Hyper-V Server 2022 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- Oracle VM VirtualBox 6.x.

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

- Microsoft SQL Server 2012 Express 64-разрядная;
- Microsoft SQL Server 2014 Express 64-разрядная;
- Microsoft SQL Server 2016 Express 64-разрядная;
- Microsoft SQL Server 2017 Express 64-разрядная;
- Microsoft SQL Server 2019 Express 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;
- Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная (требуются дополнительные действия);
- Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия);
- Microsoft Azure SQL Database;
- Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;

- MySQL 5.7 Community 32-разрядная/64-разрядная;
- MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
- MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
- MariaDB 10.5.x 32-разрядная/64-разрядная;
- MariaDB 10.4.x 32-разрядная/64-разрядная;
- MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
- MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

В программном средстве антивирусной защиты 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 Exchange ActiveSync;
- 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;
- 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;
- возможность развернуть сервер администрирования как систему высокой доступности.

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

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

- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;
- Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная;
- Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная;
- CentOS 7.x 64-разрядная;
- Red Hat Enterprise Linux Server 8.x 64-разрядная;
- Red Hat Enterprise Linux Server 7.x 64-разрядная;
- SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная;
- SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная;
- Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
- Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
- Astra Linux Common Edition 2.12 64-разрядная;
- Альт Сервер 10 64-разрядная;
- Альт Сервер 9.2 64-разрядная;
- Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
- Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная;
- Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная;
- Oracle Linux 7 64-разрядная;
- Oracle Linux 8 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

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

- VMware vSphere 6.7.
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Microsoft Hyper-V Server 2022 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:
- Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
- Альт Сервер 10 64-разрядная;
- Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная

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

- MySQL 5.7 Community 32-разрядная/64-разрядная;
- MySQL 8.0 32-разрядная/64-разрядная;
- MariaDB 10.5.x 32-разрядная/64-разрядная;
- MariaDB 10.4.x 32-разрядная/64-разрядная;
- MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
- MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

В программном средстве антивирусной защиты 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;
- создание резервной копии системы управления встроенными средствами системы управления;
- наличие системы контроля возникновения вирусных эпидемий;
- управления антивирусной защитой с использованием WEB консоли;
- возможность 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;
- возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
- возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных обеспечивают 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

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, включают документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

- «Руководство пользователя (администратора)»

Документация, поставляемая с антивирусными средствами, детально описывает процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Требования к потенциальному поставщику

Потенциальный Поставщик при подаче конкурсной документации предоставляет:

- электронные копии действующих сертификатов не менее одного специалиста второго уровня по предлагаемому программному обеспечению.
- авторизационное письмо от производителя Системы, подтверждающее наличие партнерских отношений с компанией-производителем на поставку и поддержку товара

Требования к технической поддержке

Потенциальный поставщик окажет Заказчику консультационно-техническое обслуживание по вопросам настройки и эксплуатации антивирусного программного обеспечения и обеспечит следующими возможностями:

- Техническая поддержка предоставляется на русском языке специалистами производителя антивирусного ПО и его партнеров на всей территории Республики Казахстан круглосуточно в праздничные и выходные дни по телефону, электронной почте и через Интернет в течении 1 года с даты генерации лицензий на программное обеспечение.

- Потенциальный поставщик обеспечит доступ к электронной информационной системе технической поддержки производителя программного обеспечения, включающей в себя направление запросов по конкретным проблемам через систему электронной почты.
- Доступ к вышеописанным службам открыт круглосуточно в течение всего времени оказания поддержки.
- Потенциальный Поставщик проведёт обучение не менее одного сотрудника по базовому курсу поставляемого программного продукта по утвержденной программе вендора, разработанной для авторизованных учебных центров. Обучение закреплено практическими занятиями, с предоставлением электронных методических пособий. Поставщик проведет обучение силами сертифицированного тренера, имеющего соответствующий профессиональный сертификат. По окончанию обучения потенциальный Поставщик обеспечит слушателям выдачу сертификата соответствующего образца. Обучение будет проведено в течение месяца после заключения договора.

Потенциальный поставщик произведёт инсталляцию консоли централизованного администрирования, произведет первоначальную настройку правил использования программ, устройств и веб-ресурсов.

- Потенциальный поставщик обеспечит Заказчика получением технической информации и/или дополнительных программных компонентов для преодоления и разрешения проблем и ошибок, обнаруженных в программных продуктах производителя.

- Гарантийное обслуживание и техническая поддержка программного обеспечения обеспечивается без дополнительных расходов со стороны Заказчика. Гарантийное обслуживание и техническая поддержка осуществляется по месту нахождения программного обеспечения.

Срок действия лицензии с 01 февраля 2027 года

Техникалық сипаттама

жұмыс станциялары мен серверлерді вируска қарсы қорғау бойынша бағдарламалық қамтамасыз етуге Лицензия Сатып алу бойынша.

Ұлттық стандарттардың атауы ҚР СТ ГОСТ Р 51188-2007 (ГОСТ Р 51188-98, IDT)

Антивирустық қорғаныс (АҚ) жұмыс станциялары мен серверлер желісінде тұрақты жұмыс істеуді қамтамасыз ететін корпоративтік шешім болуы керек. Бүкіл ұйым аясында бірыңғай антивирустық құралдар қолданылады.

Осы Техникалық ерекшелік антивирустық қорғау жүйесін енгізу бойынша ілеспе қызметтер көрсете отырып, жеткізілетін бағдарламалық қамтамасыз етуге қойылатын талаптарды белгілейтін іргелі құжат болып табылады. Жүйенің барлық компоненттері бір-бірімен толық интеграцияға ие.

1. Антивирустық қорғау бағдарламалық жасақтамасына қойылатын жалпы талаптар

1.1. Қорғалатын түйіндердің жалпы саны: 400 жс ;

1.2. Лицензияның жарамдылық мерзімі: бағдарламалық жасақтама лицензиялары жасалған сәттен бастап 12 ай.

1.3. Жеткізу мерзімі: шарт заңды күшіне енген күннен бастап 15 күнтізбелік күннен аспайды.

2. Вирусқа қарсы қорғау жөніндегі бағдарламалық қамтамасыз етуге қойылатын техникалық талаптар

Антивирустық құралдар:

- Windows жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама;
- MacOS жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама;
- Linux жұмыс станциялары мен серверлеріне арналған антивирустық бағдарламалық жасақтама;
- Windows файлдық серверлеріне арналған антивирустық бағдарламалық жасақтама;
- мобильді құрылғыларға (смартфондар мен планшеттерге)арналған антивирустық бағдарламалық жасақтама;
- орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары;
- жаңартылатын зиянды бағдарлама қолтаңбасы және шабуыл дерекқорлары;
- пайдалану құжаттамасы орыс тілінде.

Барлық антивирустық құралдардың, соның ішінде басқару құралдарының бағдарламалық интерфейсі орыс және ағылшын тілдерінде.

Барлық антивирустық құралдар, соның ішінде басқару элементтері орыс және ағылшын тілдерінде контекстік анықтамалық жүйеге ие.

Windows жұмыс станцияларына арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар

Антивирустық қорғаныс бағдарламалық жасақтамасы келесі нұсқалардағы жұмыс станциялары үшін операциялық жүйені басқаратын компьютерлерде жұмыс істейді:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 және одан жоғары;
- Windows 8 Professional / Enterprise (32 / 64 бит);
- Windows 8.1 Professional / Enterprise (32 / 64 бит);
- Windows 10 Home / Pro / Pro жұмыс станциялары / Education / Enterprise;
- Windows 11 Home / Pro / Pro жұмыс станциялары / Education / Enterprise үшін.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылады:

- нақты уақыт режимінде және нысанның мәтінмәндік мәзірінен сұраныс бойынша антивирустық сканерлеу;
- кесте бойынша антивирустық сканерлеу;
- қосылатын құрылғыларды антивирустық сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- белсенді инфекцияның әрекеттерін бейтараптандыру;
- қолданбаның мінез-құлқын және оның зиянды әрекеттерін анықтау және рұқсат етілмеген әрекеттерді анықтау үшін жүйеде жасаған әрекеттерін талдау;
- желі арқылы қол жетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қоңырауларды талдау;
- бағдарламалық жасақтамадағы осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, соның ішінде жүйелік процестердің жадын қорғау;
- емдеу кезінде зиянды бағдарламалық қамтамасыз ету әрекеттерін кері қайтару, оның ішінде шифрланған, зиянды бағдарламалармен, файлдармен қалпына келтіру;
- артықшылық шектеулері (тізілімге жазылу, файлдарға, қалталарға және басқа процестерге қол жеткізу, тапсырмаларды жоспарлаушыға хабарласу, құрылғыларға қол жеткізу, объектілерге құқықтарды өзгерту және т. б.) процестер мен қосымшалар үшін, сенім деңгейін анықтай отырып, динамикалық түрде жаңартылатын теңшелетін қолданбалар тізімдері;
- іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау;
- келесі форматтағы мұрағаттардағы файлдарды антивирустық тексеру және емдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- келесі хаттамалар бойынша берілетін кіріс және шығыс трафикті тексеретін зиянды бағдарламалардан электрондық поштаны қорғау: IMAP, SMTP, POP3, MAPI, NNTP;
- берілген файл түрлерінің атын өзгерту немесе жою мүмкіндігі бар пошта тіркемелерінің сүзгісі;
- https (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP хаттамалары бойынша пайдаланушының компьютеріне келіп түсетін желілік трафикті, оның ішінде эвристикалық талдау, сенімді ресурстарды теңшеу мүмкіндігі және құлыптау немесе статистика режимінде жұмыс істеу арқылы тексеру;
- жүктелетін веб-беттердегі баннерлер мен қалқымалы терезелерді бұғаттау;
- фишингтік және қауіпті сайттарды тану және бұғаттау;
- желілік сегменттерді санаттау мүмкіндігі бар бағдарламалар үшін желілік пакеттік ережелер мен желілік ережелерді құруға мүмкіндік беретін кіріктірілген желі экраны;
- кез-келген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран ережелерін қолдана отырып, желілік шабуылдардан қорғау;
- құрылғының MAC мекенжайын қолдан жасау үшін ARP протоколындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
- бірнеше желілік қосылымдарды бір уақытта орнатуды бұғаттау мүмкіндігі бар желілік көпір түріндегі желілік қосылымдарды басқару;
- барлық немесе белгілі бір пайдаланушы топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелер жасау, компонент бағдарламаларды бағдарламаны, металеректерді, сертификатты немесе оның ізін, бақылау сомасын табу жолында да, алдын ала берілген қолданба санаттары бойынша да бақылауы керек бағдарламалық жасақтама өндірушісі, компонент қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе құлыптау режимінде жұмыс істеуі керек;

- құрылғының түрі және / немесе пайдаланылатын автобус бойынша сыртқы енгізу/шығару құрылғыларымен пайдаланушының жұмысын бақылау, олардың идентификаторы бойынша сенімді құрылғылардың тізімін жасау мүмкіндігі және Active Directory ішінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігі;
- MTP құрылғыларын басқару және құрылғыларды бақылау шеңберінде барлық немесе пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін осы типтегі құрылғыларға қол жеткізу ережелерін теңшеу;
- алынбалы дискілердегі файлдарды жазу және / немесе жою туралы Оқиғалар журналына жазбалар;
- файлдық жүйесі бар құрылғыларға қол жеткізу ережелеріне басымдық беру;
- пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық жаңартылған санатқа, сондай-ақ ақпарат түріне (аудио, видео және т. б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге мүмкіндік беру, сондай-ақ оны тек белгілі бір пайдаланушыларға тағайындау. Active Directory;
- BadUSB типті шабуылдардан қорғау;
- анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтауға арналған арнайы тапсырманы іске қосыңыз.
- қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ пароль арқылы қолданба параметрлеріне кіруді қорғау;
- сенімді қашықтан басқару бағдарламалары арқылы параметрлерді басқару;
- тек таңдалған антивирустық бағдарламалық құрал компоненттерін орнату;
- бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
- тапсырмаларды кесте бойынша және/немесе қолданбаны іске қосқаннан кейін бірден іске қосыңыз;
- файл кеңістігін сканерлеу кезінде пайдаланушылардың ынғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- өткен тексеру уақытынан бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- антивирустық бағдарламаның тұтастығын тексеру;
- файлдың бақылау сомасы, аты/каталог маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу;
- ережелер мен ерекшеліктер тізімін XML форматына импорттау және экспорттау;
- антивируста жойылған вирус жұққан файлдар үшін қорғалған сақтау орны бар, оларды қалпына келтіру мүмкіндігі бар;
- антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы;
- антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ Графикалық интерфейстің жеңілдетілген нұсқасының болуы, мүмкіндіктердің минималды жиынтығы;
- Windows Defender Security Center интеграциясы;
- Antimalware Scan Interface (AMSI)қолдауының болуы;
- Linux үшін Windows Subsystem (WSL) қолдауына ие болу;
- резервтік қоймадан объектілерді қалпына келтіруді құпия сөзбен қорғаңыз;
- интернет байланысы шектеулі болған жағдайда желілік трафиктің шектеулері;
- TCP және UDP хаттамалары бойынша желіні бақылау құралының болуы;
- тексеру үзілген жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;
- орнату мүмкіндігі тапсырманың орындалу ұзақтығын шектеу;
- тексеру тапсырмаларын кезекке қою мүмкіндігі, егер тексеру қазірдің өзінде орындалса.

Windows серверлеріне арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар

Антивирустық бағдарламалық жасақтама келесі нұсқалардың файлдық серверлері үшін операциялық жүйені басқаратын компьютерлерде жұмыс істейді:

- Windows Small Business Server 2011 Essentials / Standard (64 биттік), Microsoft Small Business Server 2011 standard (64 биттік) тек Microsoft Windows Server 2008 R2 үшін Service Pack 1 орнатылған кезде ғана қолдау көрсетіледі;
- Windows MultiPoint Server 2011 (64 бит);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 және одан жоғары;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылады:

- нақты уақыт режимінде және нысанның мәтінмәндік мәзірінен сұраныс бойынша антивирустық сканерлеу;
- кесте бойынша антивирустық сканерлеу;
- қосылатын құрылғыларды антивирустық сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- белсенді инфекцияның әрекеттерін бейтараптандыру;
- қолданбаның мінез-құлқын және оның зиянды әрекеттерін анықтау және рұқсат етілмеген әрекеттерді анықтау үшін жүйеде жасаған әрекеттерін талдау;
- желі арқылы қол жетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қоныраулардың талдау;
- бағдарламалық жасақтамадағы осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, соның ішінде жүйелік процестердің жадын қорғау;
- емдеу кезінде зиянды бағдарламалық қамтамасыз ету әрекеттерін кері қайтару, оның ішінде шифрланған, зиянды бағдарламалармен, файлдармен қалпына келтіру;
- бұлтқа негізделген жаңа қауіптерден қорғау, нақты уақыт режимінде бағдарламаға немесе файлға қатысты үкім шығару үшін өндірушінің ресурстарына қол жеткізуге мүмкіндік береді;
- RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматтарындағы файлдарды антивирустық тексеру және емдеу;
- желілік сегменттерді санаттау мүмкіндігі бар бағдарламалар үшін желілік пакеттік ережелер мен желілік ережелерді құруға мүмкіндік беретін кіріктірілген желі экраны;
- құрылғының MAC мекенжайын қолдан жасау үшін ARP протоколындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
- анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтауға арналған арнайы тапсырманы іске қосыңыз.
- қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалардан, зиянкестерден немесе біліктілігі жоқ пайдаланушылардан қорғауды өшірмеу үшін пароль арқылы қолданба параметрлеріне кіруді қорғау;
- тек таңдалған антивирустық бағдарламалық құрал компоненттерін орнату;
- бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
- тапсырмаларды кесте бойынша және/немесе амалдық жүйе жүктелгеннен кейін бірден іске қосыңыз;
- файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- өткен тексеру уақытынан бері күйі өзгермеген нысандарды өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- антивирустық бағдарламаның тұтастығын тексеру;
- файлдың бақылау сомасы, аты/каталог маскасы немесе файлда сенімді шифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу;
- антивируста жойылған вирус жұққан файлдар үшін қорғалған сақтау орны бар, оларды қалпына келтіру мүмкіндігі бар;

- антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы;
- антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ Графикалық интерфейстің жеңілдетілген нұсқасының болуы, мүмкіндіктердің минималды жиынтығы;
- Windows Defender Security Center интеграциясы;
- Antimalware Scan Interface (AMSI)қолдауының болуы;
- Linux үшін Windows Subsystem (WSL) қолдауына ие болу;
- резервтік қоймадан объектілерді қалпына келтіруді құпия сөзбен қорғаңыз.
- ережелер мен ерекшеліктер тізімін XML форматына импорттау және экспорттау;
- интернет байланысы шектеулі болған жағдайда желілік трафиктің шектеулері;
- тексеру үзілген жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;
- тапсырманың орындалу ұзақтығын шектеу мүмкіндігі;
- тексеру тапсырмаларын кезекке қою мүмкіндігі, егер тексеру қазірдің өзінде орындалса.

Мас жұмыс станцияларына арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар

Мас жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істейді:

- macOS 10.14 - 12;

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылады:

- резиденттік антивирустық бақылау;
- бұлтқа негізделген жаңа қауіптерден қорғау, нақты уақыт режимінде бағдарламаға немесе файлға қатысты үкім шығару үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік береді;
- кесте бойынша антивирустық базаларды автоматты түрде жаңарту;
- қалпына келтіру мүмкіндігі үшін вирус жұққан файлдарды жоймас бұрын олардың сақтық көшірмесін жасаңыз;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- кез-келген типтегі есептеу желілерінде, соның ішінде сымсыз желілерде жұмыс істеу кезінде ең танымал қосымшаларға арналған кіруді анықтау және алдын-алу жүйесін (IDS/IPS) және желілік белсенділік ережелерін қолдана отырып, желілік шабуылдардан қорғау;
- антивирустық қорғаныс өндірушісінің беделді бұлтты қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды бұғаттау;
- Safari, Google Chrome және Firefox браузерлері арқылы берілетін желілік трафикті тексеру (HTTP және HTTPS трафигі);
- пайдаланушының Интернет желісімен жұмысын бақылау, соның ішінде санаттарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жанартылған белгілі бір ресурстарға немесе ресурстар санаттарына кіруге нақты тыйым салуды немесе рұқсатты қосу
- өткен тексеру уақытынан бері күйі өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
- жаңа kav пәрменін пайдаланып пәрмен жолынан кеңейтімдерді орнату мүмкіндігі;
- файлдық операцияларды ұстап қалу деңгейінде көрсетілген аймақтарды тексеру кезінде ерекшеліктерді орнату мүмкіндігі;
- дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнату мүмкіндігі.

Linux жұмыс станциялары мен серверлеріне арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар

Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың 32 биттік операциялық жүйелерін басқаратын компьютерлерде жұмыс істейді:

- CentOS 6.7 және одан жоғары.
- Debian GNU / Linux 10.1 және одан жоғары.
- Debian GNU/Linux 11.
- Mageia 4.
- Red Hat Enterprise Linux 6.7 және одан жоғары.
- Альт 8 СП жұмыс станциясы.
- Альт 8 СП сервері.
- Альт білім 10.
- Альт жұмыс станциясы 10.

Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың 64 биттік операциялық жүйелерімен жұмыс істейтін компьютерлерде жұмыс істейді:

- AlmaLinux OS 8 және одан жоғары.
- AlmaLinux OS 9 және одан жоғары.
- AlterOS 7.5 және одан жоғары.
- Amazon Linux 2.
- Astra Linux Common Edition 2.12.
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.5).
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.6).
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.7).
- Astra Linux Special Edition RUSB.10015-16 (орындау 1) (кезекті жаңарту 1.6).
- CentOS 6.7 және одан жоғары.
- CentOS 7.2 және одан жоғары.
- CentOS Stream 9.
- Debian GNU / Linux 10.1 және одан жоғары.
- Debian GNU/Linux 11.
- EMIAS 1.0.
- EulerOS 2.0 SP5.
- LinuxMint 19.2 және одан жоғары.
- LinuxMint 20.3 және одан жоғары.
- openSUSE Leap 15.0 және одан жоғары.
- Linacle Linux 7.3 және одан жоғары.
- Linacle Linux 8.0 және одан жоғары.
- Red Hat Enterprise Linux 6.7 және одан жоғары.
- Red Hat Enterprise Linux 7.2 және одан жоғары.
- Red Hat Enterprise Linux 8.0 және одан жоғары.
- Red Hat Enterprise Linux 9.
- Rocky Linux 8.5 және одан жоғары.
- SUSE Linux Enterprise Server 12.5 және одан жоғары.
- SUSE Linux Enterprise Server 15 және одан жоғары.
- Ubuntu 20.04 LTS.
- Ubuntu 22.04 LTS.
- Alt 8 SP жұмыс станциясы.
- Alt 8 SP сервері.
- Альт білім 10.
- Альт жұмыс станциясы 10.
- Альт Сервер 10.
- Атлант, Alcyone құрастыру, 2022.02 нұсқасы.
- Гослинукс 7.17.
- Гослинукс 7.2.

- РЕД ОС 7.3.
- РОСА "Кобальт" 7.9.
- РОСА "Хром" 12.
- ОСОН "ОСНова".

ARM архитектурасына арналған 64 биттік операциялық жүйелер:

- Astra Linux Special Edition RUSB.10152-02(кезекті жаңарту 4.7).
- EulerOS 2.0 SP8.
- SUSE Linux Enterprise Server 15 SP3.
- Ubuntu 20.04 LTS.
- Альт 8 СП сервері.
- РЕД ОС 7.3

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылады:

- резиденттік антивирустық мониторинг;
- нақты уақыт режимінде іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау;
- SMB / NFS арқылы қол жетімді ресурстарды тексеру;
- ядро жадын тексеру мүмкіндігі;
- бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор;
- пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу;
- zip мұрағаттарындағы файлдарды антивирустық тексеру; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
- электрондық пошта хабарламаларын мәтіндік форматта тексеру (Plain text);
- файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытының шегі, тексерілетін файл өлшемінің шегі, кэштеу механизмі тексерілген және тексерілгеннен кейін өзгертілмеген файлдар туралы ақпарат);
- SMB / NFS протоколдары бойынша желіге қол жетімді жергілікті каталогтардағы файлдарды кашықтан зиянды шифрлаудан қорғау;
- тексеру кезінде файлдарды бұғаттау опциясын қосыңыз;
- күдікті және бүлінген объектілерді карантинге орналастыру;
- SAMBA деңгейіндегі файлдық операцияларды ұстап алу және тексеру;
- ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару;
- тапсырмаларды кесте бойынша және/немесе амалдық жүйе жүктелгеннен кейін бірден іске қосыңыз;
- есептерді HTML және CSV форматтарында экспорттау және сақтау;
- файл кеңістігін сканерлеу кезінде пайдаланушылардың ынғайлы жұмысын камтамасыз ету үшін ДК ресурстарын пайдалануды икемді басқару;
- жұқтырған объектінің көшірмесін, егер ол ақпараттық құндылықты білдірсе, талап бойынша Объектіні ықтимал калпына келтіру максатында емдеу және жою алдында резервтік қоймада сақтау;
- түбірлік құқықтары жоқ пайдаланушы графикалық интерфейсі арқылы басқару;
- жоғарыда аталған барлық компоненттерді бірыңғай басқару жүйесі немесе веб-консоль арқылы орталықтандырылған басқару;
- пайдаланушылардың орнатылған немесе компьютерге қосылған құрылғыларға құрылғы түрлері мен қосылу шиналары бойынша қол жеткізуін басқару;
- алынбалы дискілерді тексеру;
- желілік шабуылдарға тән әрекеттің кіріс желілік трафигін бақылау
- HTTP/HTTPS және FTP протоколдары арқылы пайдаланушының компьютеріне келетін трафикті тексеру, сондай-ақ веб-мекен-жайлардың зиянды немесе фишингке жататындығын орнату мүмкіндігі;
- пайдаланушының компьютеріндегі бағдарламалардың әрекеттері туралы мәліметтер алу;
- бағдарламаны іске қосқан кезде бақылау файлдарын жасаңыз;

- компьютерлерде орнатылған бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу;
- автоматты іске қосу нысандарын тексеру, жүктеу секторлары, процесс жады және ядро жады;
- емдеу немесе жою алдында файлдардың сақтық көшірмелерін сақтау және сақтық көшірмелерден файлдарды қалпына келтіру.

Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін вируска қарсы қорғаудың бағдарламалық құралдарына қойылатын талаптар

Windows файлдық серверлеріне арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істейді:

Microsoft Windows 32 биттік операциялық жүйелер

- Windows Server 2003 Standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен;
- Windows Server 2003 R2 Foundation / Standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен;
- Windows Server 2008 standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен;
- Windows Server 2008 core standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен.

64 биттік Microsoft Windows операциялық жүйелері

- Windows Server 2003 Standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен;
- Windows Server 2003 R2 standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен;
- Windows Server 2008 core standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен;
- Windows Server 2008 standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен;
- Microsoft Small Business Server 2008 Standard / Premium SP2 немесе одан жоғары;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / datacenter SP1 немесе одан жоғары жаңарту бумасымен;
- Windows Server 2008 R2 core standard / Enterprise / datacenter SP1 немесе одан жоғары жаңарту бумасымен;
- Windows Hyper-V Server 2008 R2 SP1 немесе одан жоғары жаңарту бумасымен;
- Microsoft Small Business Server 2011 Essentials / standard SP1 немесе одан жоғары;
- Microsoft Windows MultiPoint Server 2011 Standard / Premium;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
- Microsoft MultiPoint Server 2012 Standard / Premium;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2016 MultiPoint;
- Windows Server 2016 Core Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2016;
- Windows Storage Server 2016;
- Windows Hyper-V Server 2016;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2019 Core;
- Windows Storage Server 2019;
- Windows Hyper-V Server 2019;
- Windows Server 2022;

- Windows 10 Enterprise multi-session.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылады:

- нақты уақыт режимінде және сұраныс бойынша әртүрлі функцияларды орындайтын серверлерде антивирустық сканерлеу: терминал серверлері, баспа серверлері, қолданба серверлері және домен контроллері, файл серверлері;
- пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу;
- тапсырмаларды кесте бойынша және/немесе амалдық жүйе жүктелгеннен кейін бірден іске қосыңыз;
- бұлтқа негізделген жаңа қауіптерден қорғау, нақты уақыт режимінде бағдарламаға немесе файлға қатысты үкім шығару үшін өндірушінің арнайы сайттарына жүгінуге мүмкіндік береді;
- RAR, ARJ, ZIP, CAB форматтарындағы файлдарды антивирустық тексеру және емлеу;
- файлдарды қорғау, балама файлдық жүйелер ағындары (NTFS-streams), жүктеу жазбасы, жергілікті және алынбалы дискілердің жүктеу секторлары;
- Microsoft Windows script Technologies (немесе Active Scripting) технологиялары бойынша жасалған VBScript және JScript сценарийлерінің қорғалған серверінде орындау әрекеттерін үздіксіз қадағалау, сценарийлердің бағдарламалық кодын тексеру және қауіпті деп танылғандардың орындалуына автоматты түрде тыйым салу.
- желі арқылы қол жетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қоңырауларды талдау;
- Microsoft Windows контейнерлерін тексеру;
- процесс жадындағы осалдықтарды пайдаланудан қорғау;
- бұзылған процестерді автоматты түрде аяқтау мүмкіндігі болуы керек, ал маңызды жүйелік процестер аяқталмауы керек;
- қорғалған тізімге процестерді қосыңыз;
- өткен тексеру уақытынан бері күйі өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету;
- жеке модульдерді жеке тапсырма арқылы олардың тұтастығын бұзуға тексеру;
- жеке тапсырма ретінде сервердің маңызды аймақтарын тексеру параметрлері;
- тапсырмалардың басымдылығына байланысты сервер ресурстарын антивирус пен басқа қосымшалар арасында бөлуді реттеу;
- фонда антивирустық сканерлеуді жалғастыру;
- маңызды оқиғалар туралы әкімшілерге хабарлаудың бірнеше жолдарының болуы (пошта хабарламасы, дыбыстық ескерту, қалқымалы терезе, Оқиғалар журналына жазу);
- зиянды бағдарламалардан, зиянкестерден немесе біліктілігі жоқ пайдаланушылардан қорғауды өшірмеуге мүмкіндік беретін, сондай-ақ антивирусты басқаруға тыйым салатын немесе рұқсат беретін рұқсат тізімдері арқылы қолданба мен қызмет опцияларына рөлдік қол жеткізу;
- Siem жүйелерімен интеграция;
- антивирустың жұмыс процестерінің санын қолмен көрсету;
- графикалық интерфейсті өшіру;
- қашықтан және жергілікті басқару консолінің болуы;
- пәрмен жолынан антивирус параметрлерін басқару;
- бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару;
- ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару;
- желілік шабуылдардың белгілері үшін кіріс трафигін талдауды қамтамасыз ететін желілік қауіптерден қорғау;
- бағдарлама процестерін сыртқы қауіптерден қорғауды қосыңыз немесе өшіріңіз (әдепкі бойынша функция қосылады). Функция қосылған кезде бағдарлама өзінің процестерін, сондай-ақ әкімшілік агенттің процестерін үшінші тарап процестерінің араласуынан қорғайды.

Мобильді құрылғыларды антивирустық қорғау бағдарламалық құралдарына қойылатын талаптар

Смартфондарды антивирустық қорғауға арналған бағдарламалық жасақтама келесі мобильді ОЖ - де жұмыс істейді:

- Android 5.0–13 (Go Edition қоспағанда, Android 12L қоса алғанда);
- iOS 10-16 немесе iPadOS 13-15;

Android ОЖ үшін смартфондарды антивирустық қорғау бағдарламалық құралында келесі функциялар іске асырылады:

- смартфонның файлдық жүйесін тұрақты антивирустық қорғау, антивирустық қорғаныс өндірушісінің бұлтқа негізделген беделді қызметін қолдана отырып, қосымша тексеру деңгейімен;
- құрылғының файлдық жүйесін сұраныс бойынша және кесте бойынша тексеру;
- орнатылған қолданбаларды жылдам тексеру
- антивирустық қорғаныс құралдарын өндірушінің беделді бұлтты қызметтерінің үкімдері негізінде зиянды және фишингтік сайттарды бұғаттау;
- жұқтырған объектілерді оқшаулауға арналған қойманың болуы;
- зиянды бағдарламаларды іздеу және қауіпті объектілерді жою кезінде қолданылатын антивирустық базаларды кесте бойынша жаңарту;
- көрсетілген қолданбаларды, соның ішінде алдын ала белгіленген қолданба санаттарын пайдаланып іске қосуды блоктау;
- рұқсат етілген қолданбалардың ақ тізімдерін қолдау;
- қосымшалардың іске қосылуын бақылау шеңберінде жүйелік қосымшаларды бұғаттау;
- Firebase Cloud Messaging (FCM)қызметі арқылы командалар мен хабарландыруларды жіберу;
- Wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануға тыйым салу;
- Wi-Fi желілеріне қосылу параметрлерін көрсетіңіз;
- орнатуға міндетті қосымшаларды көрсетіңіз;
- мобильді құрылғыны құлыптау, деректерді жою, жұмысқа байланысты деректерді жою, құрылғының орналасқан жерінің координаттарын алу, зауыттық параметрлерге қашықтан оралу (factory reset);
- қағидалар тізімін құру, олардың негізінде мобильді құрылғының құрылғыны автоматты түрде бұғаттау, деректерді жою, сәйкессіздіктер анықталған кезде корпоративтік қосымшаларды іске қосуға тыйым салу мүмкіндігімен корпоративтік саясатқа сәйкестігін тексеру жүзеге асырылатын болады;
- Samsung knox1 және knox2 технологияларын қолдау.
- Apple iOS ОЖ үшін смартфондарды қорғаудың бағдарламалық жасақтамасында келесі функциялар іске асырылуы керек:
- топтық саясаттарды қолдана отырып, IOS MDM құрылғыларының параметрлерін қашықтан конфигурациялау;
- деректерді блоктау және жою пәрменін жіберу;
- мобильді құрылғылардың топтық қауіпсіздік саясатын жасаңыз;
- Exchange ActiveSync\ iOS MDM протоколы арқылы қосылған құрылғылардың конфигурация параметрлерін қашықтан конфигурациялаңыз;
- пайдаланушылардың мобильді құрылғыларының жұмысы туралы есептер мен статистиканы алу;
- supervised mode пайдалану кезінде антивирустық қорғаныс құралдарын өндірушінің беделді бұлттық қызметтерінің үкімдеріне негізделген зиянды және фишингтік сайттарды бұғаттау;
- бір басқару консолі арқылы орталықтандырылған басқару;
- басқарылатын құрылғыда ITUNES, Safari немесе Game Center сияқты құрылғының жергілікті қосымшаларын пайдалануға болатындығын басқаруға мүмкіндік беретін компоненттің болуы.

Windows ОЖ негізіндегі орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істейді:

- Microsoft Windows 10 Enterprise 2015 ltsb 32 биттік / 64 биттік;

- Microsoft Windows 10 Enterprise 2016 ltsb 32 биттік / 64 биттік;
- Microsoft Windows 10 Enterprise 2019 ltsc 32 биттік / 64 биттік;
- Microsoft Windows 10 Pro RS5 (қазан 2018 жаңарту, 1809) 32 бит / 64 бит;
- Microsoft Windows 10 Pro RS5 жұмыс станциялары үшін (Қазан 2018 жаңарту, 1809) 32 бит / 64 бит;
- Microsoft Windows 10 Enterprise RS5 (қазан 2018 жаңарту, 1809) 32 биттік / 64 биттік;
- Microsoft Windows 10 Education RS5 (қазан 2018 жаңарту, 1809) 32 биттік / 64 биттік;
- Microsoft Windows 10 Pro 19H1 32 биттік / 64 биттік;
- Microsoft Windows 10 Pro 19h1 жұмыс станциялары үшін 32 биттік / 64 биттік;
- Microsoft Windows 10 Enterprise 19h1 32 биттік / 64 биттік;
- Microsoft Windows 10 Education 19h1 32 биттік / 64 биттік;
- Microsoft Windows 10 Pro 19H2 32 биттік / 64 биттік;
- Microsoft Windows 10 Pro 19h2 жұмыс станциялары үшін 32 бит / 64 бит;
- Microsoft Windows 10 Enterprise 19H2 32 биттік / 64 биттік;
- Microsoft Windows 10 Education 19h2 32 биттік / 64 биттік;
- Microsoft Windows 10 Home 20H1 (мамыр 2020 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Pro 20H1 (мамыр 2020 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Enterprise 20H1 (мамыр 2020 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Education 20H1 (мамыр 2020 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Home 20H2 (қазан 2020 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Pro 20H2 (қазан 2020 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Enterprise 20H2 (қазан 2020 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Education 20H2 (қазан 2020 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Home 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Pro 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Enterprise 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Education 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Home 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Pro 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Enterprise 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 10 Education 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит;
- Microsoft Windows 11 Home 64 биттік;
- Microsoft Windows 11 Pro 64 биттік;
- Microsoft Windows 11 Enterprise 64 биттік;
- Microsoft Windows 11 Education 64 биттік;
- Microsoft Windows 8.1 Pro 32 биттік/64 биттік;
- Microsoft Windows 8.1 Enterprise 32 биттік / 64 биттік;
- Microsoft Windows 8 Pro 32 биттік/64 биттік;
- Microsoft Windows 8 Enterprise 32 биттік / 64 биттік;
- Microsoft Windows 7 Professional Service Pack 1 32 бит / 64 бит;
- Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32 бит / 64 бит;
- Windows Server 2008 R2 with Standard Service Pack 1 және одан жоғары 64 биттік;
- Windows Server 2008 R2 Service Pack 1 (барлық басылымдар) 64 бит;
- Windows Server 2012 Server Core 64 биттік;
- Windows Server 2012 Datacenter 64 биттік;
- Windows Server 2012 essentials 64 биттік;
- Windows Server 2012 foundation 64 биттік;
- Windows Server 2012 standard 64 биттік;
- Windows Server 2012 R2 Server Core 64 биттік;
- Windows Server 2012 R2 Datacenter 64 биттік;
- Windows Server 2012 R2 Essentials 64 биттік;
- Windows Server 2012 R2 foundation 64 биттік;
- Windows Server 2012 R2 standard 64 биттік;
- Windows Server 2016 Datacenter (LTSB) 64 биттік;
- Windows Server 2016 Standard (LTSB) 64 биттік;
- Windows Server 2016 (Server Core орнату опциясы) (LTSB) 64 бит;
- Windows Server 2019 standard 64 биттік;
- Windows Server 2019 Datacenter 64 биттік;
- Windows Server 2019 Core 64 биттік;

- Windows Server 2022 standard 64 биттік;
- Windows Server 2022 Datacenter 64 биттік;
- Windows Server 2022 Core 64 биттік;
- Windows Storage Server 2012 64 бит;
- Windows Storage Server 2012 R2 64 бит;
- Windows Storage Server 2016 64 бит;
- Windows Storage Server 2019 64 биттік.

Орталықтандырылған басқару, бақылау және жанарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатылады:

- VMware vSphere 6.7;
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper - V Server 2012 64 бит;
- Microsoft Hyper - V Server 2012 R2 64 бит;
- Microsoft Hyper - V Server 2016 64 бит;
- Microsoft Hyper - V Server 2019 64 бит;
- Microsoft Hyper - V Server 2022 64 бит;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- Oracle VM VirtualBox 6.x.

Орталықтандырылған басқару, мониторинг және жанарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істейді:

- Microsoft SQL Server 2012 express 64 биттік;
- Microsoft SQL Server 2014 express 64 биттік;
- Microsoft SQL Server 2016 express 64 биттік;
- Microsoft SQL Server 2017 express 64 биттік;
- Microsoft SQL Server 2019 express 64 биттік;
- Microsoft SQL Server 2014 (барлық басылымдар) 64 бит;
- Microsoft SQL Server 2016 (Барлық басылымдар) 64 бит;
- Microsoft SQL Server 2017 (барлық басылымдар) Windows 64 биттік;
- Microsoft SQL Server 2017 (барлық басылымдар) Linux үшін 64 бит;
- Microsoft SQL Server 2019 (барлық басылымдар) Windows 64 биттік (қосымша қадамдар қажет);
- Microsoft SQL Server 2019 (барлық басылымдар) Linux үшін 64 биттік (қосымша қадамдар қажет);
- Microsoft Azure SQL Database;
- Amazon RDS және Microsoft Azure бұлттық платформаларында қолдау көрсетілетін SQL серверлерінің барлық нұсқалары;
- MySQL 5.7 Community 32 биттік / 64 биттік;
- MySQL Standard Edition 8.0 (8.0.20 және одан жоғары шығарылым) 32 бит / 64 бит;
- MySQL Enterprise Edition 8.0 (8.0.20 және одан жоғары шығарылым) 32 биттік / 64 биттік;
- MariaDB 10.5.x 32 бит / 64 бит;
- MariaDB 10.4.x 32 бит / 64 бит;
- MariaDB 10.3.22 және одан жоғары 32 биттік/64 биттік;
- MariaDB Server 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік;
- MariaDB Galera Cluster 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік;
- MariaDB 10.1.30 және одан жоғары 32 биттік/64 биттік.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылады:

- қорғалатын түйіндер санына байланысты орталықтандырылған басқару, бақылау және жанарту қондырғысының архитектурасын таңдау;
- ұйымда компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында Active Directory-дан ақпаратты оқу;
- анықталған компьютерлерді IP мекен-жайы, ОЖ түрі, OU AD-да болу ережелерінің параметрлері;

- желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтары бойынша автоматты түрде бөлу; IP мекенжайы, ОЖ типі, ou AD-да болу бойынша тасымалдау ережелерін теңшеу мүмкіндігі;
- орталықтандырылған антивирустық бағдарламалық жасақтаманы орнату, жаңарту және жою;
- орталықтандырылған орнату, әкімшілік;
- қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау;
- басқару орталығы құралдарымен үйлеспейтін қосымшаларды орталықтандырылған жою (қолмен және автоматты) ;
- саясат пен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;
- антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін-RPC, GPO, басқару жүйесінің құралдары, жергілікті орнату үшін-дербес орнату пакетін құру мүмкіндігі;
- пайдаланушы кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты антивирустық шептің параметрлерін қайта анықтайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар;
- қайта бөлу орын алатын триггерлердің иерархиялары;
- клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу;
- жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
- виртуалды машиналар желісін тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу;
- әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігімен көп деңгейлі басқару жүйесін құру;
- еркін деңгейдегі басқару серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
- басқару серверлері үшін көп жалға алуды қолдау (multi-tenancy) ;
- байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту;
- басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қол жеткізу;
- клиенттік компьютерлерге лицензияны автоматты түрде тарату;
- пайдаланушылардың компьютерлерінде орнатылған бағдарламалық жасақтама мен жабдықты түгендеу;
- орнатылған антивирустық қорғау Қосымшаларының жұмысында оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді баптау;
- Exchange ActiveSync сервері арқылы мобильді құрылғыларды басқару мүмкіндігі;
- iOS MDM сервері арқылы мобильді құрылғыларды басқару мүмкіндігі;
- берілген оқиғалар туралы SMS-хабарламаларды жіберу;
- басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату;
- басқару жүйесіне желілік жүктемені азайту үшін кез-келген ұйымның компьютерін жаңартуларды қайта жіберу орталығына бағыттау;
- ұйымның кез-келген компьютерін антивирустық агенттердің оқиғаларын бағыттау орталығы, клиенттік компьютерлердің таңдалған тобы, басқару жүйесіне желілік жүктемені азайту үшін орталықтандырылған басқару серверіне бағыттау;
- вируска қарсы қорғау оқиғалары, түгендеу деректері, белгіленген бағдарламаларды лицензиялау деректері бойынша графикалық есептерді құру;
- жүйенің жұмысы туралы алдын ала конфигурацияланған стандартты есептердің болуы;
- есептерді PDF және XML форматындағы файлдарға экспорттау;
- антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин объектілерін орталықтандырылған басқару;
- басқару серверінде аутентификация үшін ішкі есептік жазбаларды құру;
- басқару жүйесінің кірістірілген құралдарын басқару жүйесінің сақтық көшірмесін жасау;
- Windows Failover Clustering қолдауы;
- Windows certificate Authority қызметімен интеграцияны қолдау;
- пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы;
- өзіне-өзі қызмет көрсету порталы басқару агентін мобильді құрылғыға орнату, мобильді құрылғыларды қарау, құлыптау пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының

мобильді құрылғысында деректерді жою мақсатында пайдаланушыларды қосу мүмкіндігін қамтамасыз етеді;

- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- Microsoft Azure және Google Cloud бұлтты инфрақұрылымындағы кондырғылар;
- орепарі интеграциясы;
- web консолін пайдаланып антивирустық қорғауды басқару;
- әкімшілік консолінe рұқсатсыз кіру қаупін азайту үшін екі сатылы тексеру;
- пайдаланушы тіркелгісінің параметрлерін өзгерткеннен кейін қосымша аутентификацияны қолданыңыз.
- IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрау мүмкіндігі;
- әкімшілік серверді қол жетімділігі жоғары жүйе ретінде орналастыру мүмкіндігі.

Linux ОЖ негізіндегі орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқару, мониторинг және жанарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істейді:

- Debian GNU/Linux 11.x (Bullseye) 32 биттік / 64 биттік;
- Debian GNU/Linux 10.x (Buster) 32 биттік / 64 биттік;
- Debian GNU/Linux 9.x (Stretch) 32 биттік / 64 биттік;
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 бит;
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64 биттік;
- CentOS 7.x 64 бит;
- Red Hat Enterprise Linux Server 8.x 64 бит;
- Red Hat Enterprise Linux Server 7.x 64 бит;
- SUSE Linux Enterprise Server 12 (барлық жанарту бумалары) 64 бит;
- SUSE Linux Enterprise Server 15 (барлық жанарту бумалары) 64 бит;
- Astra Linux Special Edition 1.7 (жабық бағдарламалық жасақтама режимі мен мандат режимін қосқанда) 64 биттік;
- Astra Linux Special Edition 1.6 (жабық бағдарламалық жасақтама режимі мен мандат режимін қосқанда) 64 биттік;
- Astra Linux Common Edition 2.12 64 бит;
- Альт Сервер 10 64 бит;
- Альт сервері 9.2 64 бит;
- Альт 8 СП сервері (ЛКНВ.11100-01) 64 биттік;
- Альт 8 СП сервері (ЛКНВ.11100-02) 64 биттік;
- Альт 8 СП сервері (ЛКНВ.11100-03) 64 биттік;
- Linacle Linux 7 64 бит;
- Linacle Linux 8 64 бит;
- red OS 7.3 64 биттік Сервер;
- red OS 7.3 64 биттік сертификатталған басылым.

Орталықтандырылған басқару, бақылау және жанарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатылады:

- VMware vSphere 6.7.
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper - V Server 2012 64 бит;
- Microsoft Hyper - V Server 2012 R2 64 бит;
- Microsoft Hyper - V Server 2016 64 бит;
- Microsoft Hyper - V Server 2019 64 бит;
- Microsoft Hyper - V Server 2022 64 бит;

- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- ядроға негізделген Виртуалды машина. Келесі операциялық жүйелерді қолдайды:
- Альт 8 СП сервері (LKNV.11100-01) 64 биттік;
- Альт Сервер 10 64 бит;
- Astra Linux Special Edition 1.7 (жабық бағдарламалық жасақтама режимі мен мандат режимін қоспағанда) 64 биттік;
- Debian GNU/Linux 11.x (Bullseye) 32 биттік / 64 биттік;
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 бит;
- red OS 7.3 64 биттік Сервер;
- red OS 7.3 64 биттік сертификатталған басылым

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істейді:

- MySQL 5.7 Community 32 биттік / 64 биттік;
- MySQL 8.0 32 биттік / 64 биттік;
- MariaDB 10.5.x 32 бит / 64 бит;
- MariaDB 10.4.x 32 бит / 64 бит;
- MariaDB 10.3.22 және одан жоғары 32 биттік/64 биттік;
- MariaDB Server 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік;
- MariaDB 10.1.30 және одан жоғары 32 биттік/64 биттік.

Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырыл:

- орталықтандырылған антивирустық бағдарламалық жасақтаманы орнату, жаңарту және жою;
- орталықтандырылған орнату, әкімшілік;
- қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау;
- саясат пен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;
- қайта бөлу орын алатын тригтерлердің иерархиялары;
- жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
- виртуалды машиналар желісін тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу;
- әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын теншеу мүмкіндігімен көп деңгейлі басқару жүйесін құру;
- еркін деңгейдегі басқару серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
- басқару серверлері үшін көп жалға алуды қолдау (multi-tenancy) ;
- байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту;
- басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қол жеткізу;
- клиенттік компьютерлерге лицензияны автоматты түрде тарату;
- орнатылған антивирустық қорғау Қосымшаларының жұмысында оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді баптау;
- белгіленген бағдарламаларды лицензиялау деректері бойынша антивирустық қорғау оқиғалары бойынша графикалық есептерді құру;
- жүйенің жұмысы туралы алдын ала конфигурацияланған стандартты есептердің болуы;
- есептерді PDF және XML форматындағы файлдарға экспорттау;
- антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин объектілерін орталықтандырылған басқару;
- басқару серверінде аутентификация үшін ішкі есептік жазбаларды құру;
- басқару жүйесінің кірістірілген құралдарын басқару жүйесінің сақтық көшірмесін жасау;
- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- web консолін пайдаланып антивирустық қорғауды басқару;

- басқару серверіне жүктемені азайту және кәсіпорын желісіндегі деректер трафигін оңтайландыру үшін басқару сервері арқылы да, тарату нүктелері арқылы да басқарылатын құрылғыларда антивирустық базалар мен бағдарламалық модульдерді жаңарту және тарату мүмкіндігі;
- Жаңартуларды тексеру тапсырмасы арқылы жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын өнімділік пен кателерді тексеру мүмкіндігі;
- антивирустық базалар мен бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары мүмкіндігін пайдалану мүмкіндігі.

Антивирустық базаларды жаңартуға қойылатын талаптар

Жаңартылатын антивирустық мәліметтер базасы келесі функционалдық мүмкіндіктерді іске асыруды қамтамасыз етеді:

- күнтізбелік тәулік ішінде кемінде 24 рет антивирустық базаларды жаңарту ережелерін жасау;
- жаңарту жолдарының көптігі, оның ішінде-байланыс арналары бойынша және иеліктен шығарылатын электрондық ақпарат тасымалдағыштарда;
- электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру.

Пайдалану құжаттамасына қойылатын талаптар

Басқару құралдарын қоса алғанда, вирусқа қарсы қорғаудың барлық бағдарламалық өнімдері үшін пайдалану құжаттамасына мемлекеттік стандарттардың талаптарына сәйкес орыс тілінде дайындалған құжаттар, оның ішінде:

- "Пайдаланушы (әкімші) нұсқаулығы"

Антивирустық құралдармен бірге жеткізілетін құжаттама тиісті антивирустық қорғаныс құралын орнату, конфигурациялау және пайдалану процесін егжей-тегжейлі сипаттайды.

Әлеуетті өнім берушіге қойылатын талаптар

Әлеуетті өнім беруші конкурстық құжаттаманы беру кезінде мыналарды ұсынады:

- ұсынылатын бағдарламалық қамтамасыз ету бойынша кемінде екінші деңгейдегі бір маманның қолданыстағы сертификаттарының электрондық көшірмелері.
- жүйені өндірушіден тауарды жеткізуге және қолдауға өндіруші компаниямен серіктестік қатынастардың бар екендігін растайтын авторизациялық хат

Техникалық қолдауға қойылатын талаптар

Әлеуетті өнім беруші Тапсырыс берушіге антивирустық бағдарламалық қамтамасыз етуді баптау және пайдалану мәселелері бойынша консультациялық-техникалық қызмет көрсетеді және мынадай мүмкіндіктермен қамтамасыз етеді:

- Техникалық қолдауды Қазақстан Республикасының бүкіл аумағында вирусқа қарсы БҚ өндірушісінің және оның серіктестерінің мамандары тәулік бойы телефон, электрондық пошта арқылы және интернет арқылы бағдарламалық қамтамасыз етуге лицензиялар жасалған күннен бастап 1 жыл ішінде орыс тілінде ұсынады.
- Әлеуетті өнім беруші электрондық пошта жүйесі арқылы нақты мәселелер бойынша сұрауларды жіберуді қамтитын бағдарламалық жасақтама өндірушісінің техникалық қолдауының электрондық ақпараттық жүйесіне қол жеткізуді қамтамасыз етеді.
- Жоғарыда сипатталған қызметтерге қол жеткізу қолдау көрсетудің барлық уақыты ішінде тәулік бойы ашық.
- Әлеуетті өнім беруші уәкілетті оқу орталықтары үшін әзірленген вендордың бекітілген бағдарламасы бойынша жеткізілетін бағдарламалық өнімнің базалық курсы бойынша кемінде төрт қызметкерді оқытуды жүргізеді. Оқыту электронды әдістемелік құралдарды ұсына отырып, практикалық сабақтармен бекітілген. Жеткізуші оқытуды тиісті кәсіби сертификаты бар

сертификатталған жаттықтырушының күшімен жүргізеді. Оқу аяқталғаннан кейін әлеуетті өнім беруші тыңдаушыларға тиісті үлгідегі сертификат беруді қамтамасыз етеді. Оқыту шарт жасалғаннан кейін бір ай ішінде жүргізіледі.

Әлеуетті жеткізуші орталықтандырылған басқару консолін орнатады, бағдарламаларды, құрылғыларды және веб-ресурстарды пайдалану ережелерін бастапқы конфигурациялайды.

- Әлеуетті Жеткізуші Тапсырыс берушіге өндірушінің бағдарламалық өнімдерінде кездесетін мәселелер мен қателерді жеңу және шешу үшін техникалық ақпаратты және/немесе қосымша бағдарламалық компоненттерді алуды қамтамасыз етеді.

- Кепілдік қызмет көрсету және бағдарламалық қамтамасыз етуді техникалық қолдау Тапсырыс беруші тарапынан қосымша шығындарсыз қамтамасыз етіледі. Кепілдік қызмет көрсету және техникалық қолдау бағдарламалық қамтамасыз етудің орналасқан жері бойынша жүзеге асырылады.

Лицензияның басталу мерзімі 2027 жыл 01 ақпан.