ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Наименование поставляемых товаров

Продление лицензии, неисключительного права на использование программного обеспечения лаборатории Касперского Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition, 100 лицензий на 1 год.

Цель и условия приобретения товаров

Целью приобретения товаров по настоящему техническому заданию является антивирусная защита оборудования, локальной сети, Интернет и программного обеспечения, находящегося в эксплуатации Заказчика.

Сведения о действующей лицензии:

Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition

№ лицензии: 13C8-161108-123500-473-677

Срок действия текущей лицензии с 02.08.2018 по 02.08.2019 г. г.

Наименование и количество приобретаемых товаров

№ п/п	Наименование	Единица измерения	Количество
1.	Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition	шт.	100

Общие требования

Антивирусные средства должны включать:

- Программные средства антивирусной защиты для рабочих станций Windows.
- Программные средства антивирусной защиты для рабочих станций MacOS.
- Программные средства антивирусной защиты для рабочих станций Linux.
- Программные средства антивирусной защиты для файловых серверов Windows.
- Программные средства антивирусной защиты для файловых серверов Linux.
- Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных 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, должен быть на русском языке.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке.

Требования к программным средствам антивирусной защиты для рабочих станций Windows

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

- Microsoft Windows XP Professional SP3 и выше x86;
- Microsoft Windows Vista SP2 и выше x86 /x64;
- Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64;
- Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 и выше x86 / x64;
- Microsoft Windows 8 Professional / Enterprise x86 / x64;
- Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
- Microsoft Windows 10 Pro / Enterprise x86 / x64;
- Microsoft Windows Embedded Standard 7 SP1 x86 / x64;
- Microsoft Windows Embedded POSReady 7 x86 / x64;
- Microsoft Windows Embedded 8.0 Standard x64;
- Microsoft Windows Embedded 8.1 Industry Pro x64.

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:

- Антивирусное сканирование в режиме реального времени и по запросу.
- Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.
- Антивирусное сканирование по расписанию.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.
- Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем.

• Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу.

• Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP — независимо от используемого почтового клиента;

• Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных сайтов.

• Блокировка баннеров и всплывающих окон загружаемых с Web-страниц.

• Распознавание и блокировка фишинг-сайтов.

• Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами.

• Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения. Возможность совершить откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных вредоносными программами файлов.

• Возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы.

• Наличие механизмов защиты от атак типа BadUSB.

• Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ.

• 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.

• Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме MD5, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory.

• Осуществление 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.

• Осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки

определенного типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory.

• Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.

• Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

• Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.

• Защита 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.

• Возможность установки только выбранных компонентов программного средства антивирусной защиты.

• Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для рабочих станций Mac

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

- Mac OS X 10.11 (El Capitan)
- Mac OS X 10.10 (Yosemite)
- Mac OS X 10.9 (Mavericks)
- Mac OS X 10.8 (Mountain Lion)
- Mac OS X 10.7 (Lion)

Программные средства антивирусной защиты для рабочих станций Mac должны обеспечивать реализацию следующих функциональных возможностей:

- Резидентный антивирусный мониторинг.
- Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.
- Антивирусное сканирование по команде пользователя или администратора и по расписанию.
- Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
- Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

- Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу.
- 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.
- Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS.
- Автоматическое обновление антивирусных баз по расписанию
- Защита информации, передаваемой через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик)

Требования к программным средствам антивирусной защиты для рабочих станций Linux

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

- Canaima 3 x32/x64
- Red Flag Desktop 6.0 SP2 x32/x64
- Red Hat Enterprise Linux 5.8 Desktop x32/x64
- Red Hat Enterprise Linux 6.2 Desktop x32/x64
- Fedora 16 x32/x64
- CentOS-6.2 x32/x64
- SUSE Linux Enterprise Desktop 10 SP4 x32/x64
- SUSE Linux Enterprise Desktop 11 SP2 x32/x64
- openSUSE Linux 12.1 x32/x64
- openSUSE Linux 12.2 x32/x64
- Debian GNU/Linux 6.0.5 x32/x64
- Mandriva Linux 2011 x32
- Ubuntu 10.04 LTS x32/x64

- Ubuntu 12.04 LTS x32/x64

Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:

- Резидентный антивирусный мониторинг.
- Проверка ресурсов доступных по SMB/ CIFS/ NFS
- Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.
- Антивирусное сканирование по команде пользователя или администратора и по расписанию.
- Антивирусная проверку и лечение файлов в архивах.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.
- Помещение подозрительных и поврежденных объектов на карантин.
- Возможность экспортировать и сохранять отчеты в форматах HTML и CSV.
- Возможность перехвата и проверки файловых операций на уровне SAMBA.
- 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.
- Возможность управления через пользовательский графический интерфейс.
- Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Windows

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

- Microsoft Windows Small Business Server 2011 Essentials / Standard x64;
- Microsoft Windows Server 2003 Standard/Enterprise SP2 x32/x64;
- Microsoft Windows Server 2003 R2 Standard/Enterprise Edition SP2 R2 x32/x64;
- Microsoft Windows Server 2008 Standard/Enterprise SP2 x32/x64;
- Microsoft Windows Server 2008 R2 x64 Standard/Enterprise;
- Microsoft Windows Server 2008 R2 x64 Standard/Enterprise SP1;

- Microsoft Windows Server 2012 Foundation x64;
- Microsoft Windows Server 2012 Standard x64;
- Microsoft Windows Server 2012 R2 Standard x64 Edition.

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

- Антивирусное сканирование в режиме реального времени и по запросу.
- 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.
- Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ
- 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.
- Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем.
- Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
- Настройки проверки критических областей сервера в качестве отдельной задачи.
- Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность 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).
- Защита 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.
- Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Linux

Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Red Hat Enterprise Linux 6.5, 6.6, 6.7, 7.2 x32/x64;
- CentOS 6.5, 6.6, 6.7 x32/x64;
- CentOS 7.2 x64;
- SUSE Linux Enterprise Server 11 SP3/SP4 x32/x64;
- SUSE Linux Enterprise Server 12 x64;
- SUSE Linux Enterprise Server 12 SP1 x64;
- Novel Open Enterprise Server 11 SP2 x64;
- Novel Open Enterprise Server 2015;
- Ubuntu Server 12.04.5 LTS x32/x64;
- Ubuntu Server 14.04 LTS x32/x64;
- Ubuntu Server 15.10 LTS x32/x64;
- Oracle Linux 7.2 x64;
- Debian GNU/Linux 7.9/8.2 x32/x64;
- OpenSuse 13.1 x32/x64;
- OpenSuse 13.2 x32/x64;
- OpenSuse LEAP 42.1 x64;
- GosLinux 6.6 x32/x64;
- Linux Mint 17.3 x64.

Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:

- Резидентный антивирусный мониторинг.
- Антивирусное сканирование по команде пользователя или администратора и по расписанию.
- Проверка ресурсов доступных по SMB/ CIFS/ NFS
- Антивирусная проверка и лечение файлов в архивах.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.

- Помещение подозрительных и поврежденных объектов на карантин.
- Формирование отчетов в форматах HTML, CSV, PDF и XLS.
- Возможность перехвата и проверки файловых операций на уровне SAMBA.
- Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.
- Удаленно через веб-браузер управлять антивирусом и настраивать его.
- Централизованно управляться с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows

Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2008 Core/Standard/ Enterprise / DataCenter SP1 и выше;
- Microsoft Windows Server 2008 R2 Core/ Standard/ Enterprise / DataCenter SP1 и выше;
- Microsoft Windows Server 2012 Core/Standard/ Essential/ DataCenter/Foundation;
- Microsoft Windows Server 2012 R2 Core/Standard/ Essential/ DataCenter/Foundation;
- Microsoft Windows Server 2016 TP4;
- Microsoft Windows Storage Server 2008 R2;
- Microsoft Windows Storage Server 2008 R2 SP2 Standard Edition;
- Microsoft Windows Storage Server 2008 R2 SP2 Workgroup Edition;
- Microsoft Windows Storage Server 2012;
- Microsoft Windows Storage Server 2012 R2;
- Microsoft Windows Hyper-V Server 2012;
- Microsoft Windows Hyper-V Server 2012 R2.

Терминальные серверы:

- Microsoft Terminal Services на базе Windows Server 2008;
- Microsoft Terminal Services на базе Windows Server 2012;
- Microsoft Terminal Services на базе Windows Server 2012 R2;
- Citrix XenApp 6.0/6.5/7.0/7.5/7.6;

- Citrix XenDeskTop 7.0/7.1/7.5/7.6.

Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

- Осуществление антивирусной проверки на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов.

- Возможность использования для защиты кластера серверов.

- Проверка следующих объектов защищаемого сервера при доступе к ним: Файлов при их записи и считывании; Альтернативных потоков файловых систем (NTFS-streams); Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей.

- Предотвращение вирусных эпидемий за счет фиксации возникновения вирусных атак.

- Восстановление после заражения путем удаления всех связанных с ликвидированным вредоносным объектом записей в системных файлах и реестре ОС, что предотвращает возможные сбои в работе 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.

- 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.

- Возможность блокировки доступа удаленного компьютера к сетевым ресурсам сервера.

- Отслеживание попыток вредоносного шифрования файлов на общих сетевых папках сервера и блокирование компьютеров с которых идет такая активность.

- Проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере.

- Проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи.

- Помещение подозрительных и поврежденных объектов на карантин. Возможность восстановления файлов из карантина в сетевые папки.

- При защите терминальных серверов поддержка режимов публикации рабочего стола и публикации приложений.

- Масштабируемость за счет задания количества рабочих процессов антивируса для ускорения обработки запросов к серверу при использовании многопроцессорных серверов.

• Балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: антивирусная проверка может продолжаться в фоновом режиме.

• Выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие)

• Наличие локальной консоли управления. Возможность подключения к другим средствам защиты для серверов масштаба предприятия с помощью локальной консоли.

• Разделение прав администраторов, основанное на стандартных механизмах ОС Microsoft Windows.

• Наличие встроенных исключений для стандартных ролей сервера (Контролер домена, Сервер БД и тд).

• Уведомления различными методами администраторов и пользователей о событиях в антивирусной защите. Поддержка Simple Network Management Protocol (SNMP).

• Поддержка технологий ReFS(Resilient file system) и CSV (Cluster Shared Volume).

• Централизованно управляться с помощью единой системы управления.

Требования к программным средствам антивирусной защиты мобильных устройств

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

• Android 4.0 – 6.0;

• Apple iOS 7.0 – 9.0;

• Windows Phone 8.1, 10.

Решение должно централизованно управлять с помощью единой консоли управления.

Программные средства для антивирусной защиты смартфонов для ОС Android должны обеспечивать следующую функциональность:

• Постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки на репутационных облачных сервисам производителя антивирусных средств защиты.

• Мгновенная проверка устанавливаемых приложений.

• Проверка файловой системы устройства по требованию и по рассписанию.

• Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты. Поддержка белых списков разрешенных сайтов.

• 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.

- Возможность получения политик безопасности через Google Cloud Messaging.

- Базовая поддержка Android for Work.

- Наличие возможности создания специальной оболочки для мобильных программ с целью контроля действий программы, возможностью удаления данных и настроек программы, добавления дополнительного пароля для старта приложения, в том числе с помощью учетных данных Active Directory .

- Возможность заблокировать wi-fi и bluetooth модули, а так же использование камеры мобильного устройства.

- Указание параметров подключения к wi-fi сетям.

- Наличие возможности указания обязательных к установке приложений.

- Блокирование нежелательных SMS сообщений.

- возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset).

- Постоянная проверка телефона на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий.

- Возможность получения текущего номера SIM-карты телефона посредством CMC, возможность автоматической блокировки устройства при смене SIM-карты или при включении телефона без SIM-карты.

- Поддержка технологий Samsung KNOX1 и KNOX2.

Программные средства для антивирусной защиты смартфонов для ОС Apple iOS должны обеспечивать следующую функциональность:

- Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты.

- Наличие возможности создания специальной оболочки для мобильных программ с целью контроля действий программы, возможностью удаления данных и настроек программы, добавления дополнительного пароля для старта приложения, в том числе с помощью учетных данных Active Directory.

Программные средства для антивирусной защиты смартфонов для ОС Windows Phone должны обеспечивать следующую функциональность:

- Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты.
- Возможность определения местоположения устройства.

Требования к программным средствам централизованного управления, мониторинга и обновления

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

- Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64;
- Microsoft Windows 8 Professional / Enterprise x86 / x64;
- Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
- Microsoft Windows 10 x86 / x64;
- Microsoft Windows Server 2008 x86 / x64;
- Microsoft Windows Server 2008 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2;
- Microsoft Windows Small Business Server 2008;
- Microsoft Windows Small Business Server 2011.

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

- Microsoft SQL Express 2005/2008/2008R2/2012/2014;
- Microsoft SQL Server 2005/2008/2008R2/2012/2014;
- Microsoft Azure SQL Database;
- MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91;
- MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90.

Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий:

- VMware Workstation 9.x, Workstation 10.x;
- VMware vSphere 5.5; Workstation 6;

- Microsoft Hyper-V: 2008, 2008 R2, 2012, 20012 R2;
- Microsoft VirtualPC 2007;
- Parallels Desktop 7 и выше;
- CitrixXenServer 6.1, 6.2;
- Oracle VM VirtualBox 4.0.4-70112.

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:

- Установка системы управления антивирусной защиты из единого дистрибутива.
- Выбор установки в зависимости от количества защищаемых узлов.
- Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.
- Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.
- 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 OUAD.
- Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.
- Централизованное удаление(ручное и автоматическое) несовместимых приложений средствами центра управления.
- Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки.
- Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему , текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности. Должна быть реализована возможность поддержки иерархии таких триггеров.
- Автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.
- 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.

- Автоматическое развертывание по требованию специализированной системы защиты для виртуальных инфраструктур на базе VMware ESXi, Microsoft Hyper-V, Citrix XenServer .

- Построение многоуровневой системы управления с возможностью настройки ролей 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.

- Возможность отправки SMS-оповещений о заданных событиях.

- Централизованная установка приложений на управляемые мобильные устройства.

- Централизованная установка сертификатов на управляемые мобильные устройства.

- Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.

- Возможность 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 как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд.

- 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 веб-консоли управления приложением.
- Наличие портала самообслуживания пользователей. Портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя.
- Наличие системы контроля возникновения вирусных эпидемий.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- Регламентное обновление 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, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

- Руководство пользователя (администратора).

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

Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

- Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.
- Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов.