

Техническая спецификация закупаемых услуг по продлению лицензий на право использования программного обеспечения

Наименование кода Единого номенклатурного справочника товаров, работ, услуг*	582950.000.000000
Наименование услуги*	Услуги по продлению лицензий на право использования программного обеспечения
Единица измерения*	Одна услуга
Количество (объем)*	1
Срок оказания услуги*	В течении 16 календарных дней с момента подачи заявки Заказчиком
Гарантийный срок (в месяцах)	Не менее 12
Описание требуемых характеристик, параметров и иных исходных данных:	Цель закупки: Продление действующей лицензии антивирусного программного обеспечения Kaspersky Security for Business EDR Оптимальный на 250 устройств сроком на 12 месяцев 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 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, должен быть на русском и английском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке. Требования к программным средствам антивирусной защиты для рабочих станций Windows Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий: - о Windows 7 Home / Professional / Ultimate /

	Enterprise Service Pack 1 и выше; - о Windows 8 Professional / Enterprise (32 / 64-разрядная); - о Windows 8.1 Professional / Enterprise (32 / 64-разрядная); - о Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise/Enterprise multi-session; - о Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise В программном средстве антивирусной защиты должны быть 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; • 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; • 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
--	--

	• настроить доступ пользователей к мобильным устройствам в приложении iTunes; • запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • полnodисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановления зашифрованного содержимого в случае сбоя загрузочного агента или файлов ОС, поддержка UEFI-систем; • поддержка двухфакторной аутентификации при полnodисковом шифровании; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля; • шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации; • возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий) • возможность создавать служебную учетную запись агента аутентификации при шифровании диска; • поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полnodисковом шифровании; • возможность настроить исключения и ограничить доступ ко всем Bluetooth-устройствам кроме устройств ввода; • возможность обновления приложения без перезагрузки операционной системы; • возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО; • возможность запретить внешнее управление службами приложения. Требования к программным средствам антивирусной защиты для серверов Windows Программные средства антивирусной защиты
--	---

	должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий: - о 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; - о Windows MultiPoint Server 2011 (64-разрядная); - о Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше; - о Windows Server 2012 Foundation / Essentials / Standard / Datacenter; - о Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; - о Windows Server 2016 Essentials / Standard / Datacenter; - о Windows Server 2019 Essentials / Standard / Datacenter; - о Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая Core Mode) В программном средстве антивирусной защиты должны быть 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; • 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; • создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же 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; • запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям; • поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов. • 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; • обновление без перезагрузки системы; • настройки прав доступа (чтение / запись) для портативных устройств (MTP), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам; • заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству
--	---

	запрещен; • настроить права печати для пользователей; • наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi; • наличие совместимости с Azure WVD; • возможность обновления приложения без перезагрузки операционной системы; • возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО. • возможность запретить внешнее управление службами приложения. • возможность использования предустановленных исключений из проверки и доверенных приложений, предназначенных для быстрой настройки доверенной зоны для работы приложения на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. 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: - о macOS 11 - 15; В программном средстве антивирусной защиты должны быть 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 вышеуказанными компонентами с помощью единой системы управления. • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault; • 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; • ограничивать загрузку процессора приложением при выполнении задач поиска вредоносного ПО; • включения облачного режима и использования облегченной версии баз вредоносного ПО, для снижения нагрузки на ресурсы операционной системы; • пропускать сканирование системного тома, доступного только для чтения, во время выполнения задач проверки по требованию; • анализировать активность приложений в операционной системе с использованием шаблонов опасного поведения (BSS); • установки из файла .pkg через JAMF; • автоматическое сканирование внешних дисков при их подключении; • поддержки клиентских сертификатов. Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 32-битных операционных систем следующих версий:
--	--

	- o Debian GNU/Linux 11.0 и выше. - o Debian GNU/Linux 12.0 и выше. - o Mageia 4. - o Альт 8 СП Рабочая Станция (8.4). - o Альт 8 СП Сервер (8.4). - o Альт Образование 10. - o Альт Рабочая Станция 10. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий: - o AlmaLinux OS 8 и выше. - o AlmaLinux OS 9 и выше. - o AlterOS 7.5 и выше. - o Amazon Linux 2. - o Astra Linux Common Edition 2.12. - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) - o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6). - o Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6). - o Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7). - o CentOS 7.2 и выше. - o CentOS Stream 8. - o CentOS Stream 9. - o Debian GNU/Linux 11.0 и выше. - o Debian GNU/Linux 12.0 и выше. - o EMIAS 1.0 и выше. - o EulerOS 2.0 SP10. - o Kylin 10. - o Linux Mint 20.3 и выше. - o Linux Mint 21.1 и выше. - o openSUSE Leap 15.0 и выше. - o Oracle Linux 7.3 и выше. - o Oracle Linux 8.0 и выше. - o Oracle Linux 9.0 и выше. - o Red Hat Enterprise Linux 7.2 и выше. - o Red Hat Enterprise Linux 8.0 и выше. - o Red Hat Enterprise Linux 9.0 и выше. - o Rocky Linux 8.5 и выше. - o Rocky Linux 9.1. - o SberLinux 8.8 (Dykhtau). - o SberLinux 8.9. - o SberOS 3.2.0. - o SUSE Linux Enterprise Server 12.5 и выше.
--	--

	- o SUSE Linux Enterprise Server 15 и выше. - o Ubuntu 20.04 LTS. - o Ubuntu 22.04 LTS. - o Ubuntu 24.04 LTS. - o Альт 8 СП Рабочая станция (8.4). - o Альт 8 СП Сервер (8.4). - o Альт Образование 10.1. - o Альт Рабочая Станция 10.1. - o Альт Сервер 10.1. - o Альт СП Рабочая Станция релиз 10. - o Альт СП Сервер релиз 10. - o Атлант, сборка Alcyone, версия 2022.02. - o Гослинукс 7.17. - o Гослинукс 7.2. - o МСВСФЕРА АРМ 9.2 и выше. - o МСВСФЕРА СЕРВЕР 9.2 и выше. - o РЕД ОС 7.3. - o РЕД ОС 8.0. - o РОСА "Кобальт" 7.9. - o РОСА "Хром" 12. - o СинтезМ-Клиент 8.6. - o СинтезМ-Сервер 8.6. Поддерживаемые 64-битные операционные системы для архитектуры ARM: - o Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7). - o CentOS Stream 9. - o EulerOS 2.0 SP10. - o SUSE Linux Enterprise Server 15. - o Ubuntu 22.04 LTS. - o Альт 8 СП Рабочая Станция (8.4). - o Альт 8 СП Сервер (8.4). - o Альт СП Рабочая Станция релиз 10. - o Альт СП Сервер релиз 10. - o РЕД ОС 7.3. - o РЕД ОС 8.0. В программном средстве антивирусной защиты должны быть 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 проверку файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .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; • получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация); • 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; • исключения процессов из проверки памяти процессов в общих параметрах программы; • оптимизировать проверку журналов работы программ с помощью параметра <code>SkipPlainTextFiles</code>; • исключения трафика из проверки программой; • использовать формат JSON для запросов и вывода информации, а также для экспорта и импорта параметров программы и параметров задач; • установки и работы на устройствах с операционными системами для архитектуры Arm; • работать в режиме информирования пользователя в случае обнаружения угроз или при обнаружении попытки доступа к устройству; • возможность управлять запуском приложений на защищаемых устройствах с помощью правил контроля в режимах списка запрещенных или разрешенных приложений; • автоматический перезапуск приложения при обновлении; • возможность задать ограничение на использование ресурсов процессора; • возможность в автоматическом режиме выключить компоненты защиты и задачи проверки при запуске приложения после установки; • уведомления пользователя о работе компонентов и задач в графическом пользовательском интерфейсе; • возможность читать память процессов, не останавливая их (ядра Linux начиная с версии 3.4); • возможность управлять доступом пользователей к веб-ресурсам;
--	--

	• функция мониторинга стабильности собственной работы приложения. Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: 32-разрядных операционных систем Microsoft Windows - o Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; - o Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; - o Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; - o Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше. 64-разрядных операционных систем Microsoft Windows - o Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; - o Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; - o Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; - o Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; - o Microsoft Small Business Server 2008 Standard / Premium SP2 или выше; - o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; - o Windows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; - o Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше; - o Microsoft Small Business Server 2011 Essentials / Standard SP1 или выше; - o Microsoft Windows MultiPoint Server 2011 Standard / Premium; - o Windows Server 2012 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter; - o Microsoft MultiPoint Server 2012 Standard /
--	--

	Premium; - o Windows Storage Server 2012; - o Windows Hyper-V Server 2012; - o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; - o Windows Storage Server 2012 R2; - o Windows Hyper-V Server 2012 R2; - o Windows Server 2016 Essentials / Standard / Datacenter; - o Windows Server 2016 MultiPoint; - o Windows Server 2016 Core Standard / Datacenter; - o Microsoft Windows MultiPoint Server 2016; - o Windows Storage Server 2016; - o Windows Hyper-V Server 2016; - o Windows Server 2019 Essentials / Standard / Datacenter; - o Windows Server 2019 Core; - o Windows Storage Server 2019; - o Windows Hyper-V Server 2019; - o Windows Server 2022; - o Windows 10 Enterprise multi-session. В программном средстве антивирусной защиты должны быть 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 эксплуатации 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. • контроль устройств, в том числе сетевых карт и модемов; • веб-контроль; • защита от почтовых угроз (плагин для Outlook); • защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления; • создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп); • создания специальных правил должно контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме; • создания специальных правил должно работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должно иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы; • осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory; • осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем; • информирование администратора о
--	--

	подключении внешних устройств; • наличие механизмов автоматической генерации правил для контроля устройств и приложений; Требования к программным средствам антивирусной защиты мобильных устройств Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС: - о Android 5.0 и выше (включая Android 12L, исключая Go Edition); - о iOS 10 и выше или iPadOS 13 и выше; В программном средстве антивирусной защиты смартфонов для ОС Android должны быть 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; • указать разрешенные версии приложений при создании правил Контроля приложений для Android-устройств. В программном средстве защиты смартфонов для ОС Apple iOS должны быть 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. • запретить изменение настроек Bluetooth для iOS MDM-устройств Требования к программным средствам расследования атак и реагирования для рабочих станций и серверов Windows Программные средства расследования атак и реагирования для рабочих станций и серверов должны поставлять в виде встроенного специализированного агента в состав антивирусного решения разработчика и обеспечивать реализацию следующих
--	---

	функциональных возможностей: • совместимость агента с антивирусными решениями разработчика программного средства; • Поддержку установки на следующие ОС: - o Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше; - o Windows 8 Professional / Enterprise (32 / 64-разрядная); - o Windows 8.1 Professional / Enterprise (32 / 64-разрядная); - o Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise/Enterprise multi-session; - o Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise - o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше; - o Windows Server 2012 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2016 Essentials / Standard / Datacenter; - o Windows Server 2019 Essentials / Standard / Datacenter; - o Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая Core Mode) • предоставлять расширенную информацию по новым обнаружениям от антивирусного решения разработчика программного средства в виде: - o графа цепочки развития угрозы; - o информации об устройстве, на котором обнаружена угроза, включающей IP-адрес, MAC, версию ОС, имя устройства, список пользователей; - o общей информации об обнаружении, включающей время обнаружения, имя объекта, параметры запуска объекта при их наличии, каталог нахождения объекта, его контрольные суммы MD5 и SHA256, имя учетной записи, режим обнаружения(например, обнаружение при сканировании по требованию или при автоматическом сканировании); - o ссылки на веб-ресурс разработчика(Threat Intelligence) для просмотра расширенной информации по объекту обнаружения; - o изменений в реестре, информации о созданных файлах, запущенных процессах, сетевых соединениях связанных с обнаружением; - o принятых антивирусным решением
--	---

	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; • установки ограничение длительности выполнения задачи; • возможность ставить задачи проверки в очередь, если проверка уже выполняется; • наличие функции Анти-Бриджинг для запрета рабочей станции одновременно устанавливать сетевые соединения по разным каналам передачи информации (проводной и беспроводной) для предотвращения создание сетевых мостов; • обновление без перезагрузки системы; • настройки прав доступа (чтение / запись) для портативных устройств (MTP), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам; • настроить доступ пользователей к мобильным устройствам в приложении Android Debug Bridge (ADB); • заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен; • настроить права печати для пользователей; • наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi; • наличие совместимости с Azure WVD;
--	--

	разработчика программного средства ответных действий. • обеспечивать возможность реагирования на выявленные угрозы из карточки инцидента, на основе автоматизированного выполнения следующих задач и применение политик для искомого устройства либо сразу для группы устройств: - о изолировать устройство, на котором произошел алерт; - о поместить файл на карантин; - о создать задачу Поиска ИОС; - о запретить запуск обнаруженного файла; - о завершение процесса на устройстве; - о запуск процесса на устройстве; - о получение файла; - о удаление файла. • обеспечивать возможность реагирования на выявленные угрозы при обнаружении индикаторов компрометации(ИОС) для искомого устройства либо сразу для группы устройств: - о сетевая изоляция устройства; - о запускать проверку важных областей; - о копию поместить на карантин, объект удалить; • поддерживать возможность формирования индикаторов компрометации(ИОС) из обнаружения, сделанного антивирусным решением разработчика для последующего сканирования на устройствах на основе следующих объектов: - о описание файлов(контрольная сумма/расположение файла); - о пути и ключи реестра; • поддерживать экспорт и импорт индикаторов компрометации(ИОС) в формате OpenИОС; • детали обнаружения должны содержать информацию о группе доверия, цифровой подписи, данные о распространении файла • запуск файлов в облачной изолированной среде для выявления вредоносной активности и возможность включения отдельного счетчика для этой технологии. • наличие подсказок к функциям реагирования на угрозы. • наличие пошаговой инструкции по обеспечению безопасности инфраструктуры организации при обнаружении индикаторов компрометации • создавать специальную задачу для осуществления сканирования заданных областей на устройстве или группе устройств по
--	--

	заданным индикаторам компрометации(IOC) по расписанию или по требованию с возможность просмотра результатов сканирования; • поддерживать все описанные сценарии работы с решением через веб-интерфейс средства централизованного управления. Требования к программным средствам расследования атак и реагирования для рабочих станций Mac Программные средства расследования атак и реагирования для рабочих станций и серверов должны поставлять в виде встроенного специализированного агента в состав антивирусного решения разработчика и обеспечивать реализацию следующих функциональных возможностей: • совместимость агента с антивирусными решениями разработчика программного средства; • Поддержку установки на следующие ОС: - о macOS 12-15; • предоставлять расширенную информацию по новым обнаружениям от антивирусного решения разработчика программного средства в виде: - о информации об устройстве, на котором обнаружена угроза, включающей IP-адрес, MAC и версию ОС; - о общей информации об обнаружении, включающей время обнаружения, имя объекта, параметры запуска объекта при их наличии, каталог нахождения объекта, его контрольные суммы MD5 и SHA256, имя учетной записи, режим обнаружения(например, обнаружение при сканировании по требованию или при автоматическом сканировании); - о ссылки на веб-ресурс разработчика(Threat Intelligence) для просмотра расширенной информации по объекту обнаружения; - о изменений в реестре, информации о созданных файлов, запущенных процессов, сетевых соединениях связанных с обнаружением; - о принятых антивирусным решением разработчика программного средства ответных действий. • обеспечивать возможность реагирования на выявленные угрозы из карточки инцидента, на основе автоматизированного выполнения следующих задач и применение политик для искомого устройства либо сразу для группы устройств: - о изолировать устройство, на котором произошел алерт; - о поместить файл на карантин;
--	---

	- о создать задачу Поиска IOC; - о запретить запуск обнаруженного файла; - о завершение процесса на устройстве; - о запуск процесса на устройстве; - о получение файла; - о удаление файла. • обеспечивать возможность реагирования на выявленные угрозы при обнаружении индикаторов компрометации(IOC) для искомого устройства либо сразу для группы устройств: - о сетевая изоляция устройства; - о запускать проверку важных областей; - о копию поместить на карантин, объект удалить; • поддерживать возможность формирования индикаторов компрометации(IOC) из обнаружения, сделанного антивирусным решением разработчика для последующего сканирования на устройствах на основе следующих объектов: - о описание файлов(контрольная сумма/расположение файла); - о пути и ключи реестра; • поддерживать экспорт и импорт индикаторов компрометации(IOC) в формате OpenIOC; • детали обнаружения должны содержать информацию о группе доверия, цифровой подписи, данные о распространении файла • запуск файлов в облачной изолированной среде для выявления вредоносной активности и возможность включения отдельного счетчика для этой технологии. • наличие подсказок к функциям реагирования на угрозы. • наличие пошаговой инструкции по обеспечению безопасности инфраструктуры организации при обнаружении индикаторов компрометации • создавать специальную задачу для осуществления сканирования заданных областей на устройстве или группе устройств по заданным индикаторам компрометации(IOC) по расписанию или по требованию с возможностью просмотра результатов сканирования; • поддерживать все описанные сценарии работы с решением через веб-интерфейс средства централизованного управления. Требования к программным средствам расследования атак и реагирования для рабочих станций и серверов Linux Программные средства расследования атак и реагирования для рабочих станций и серверов
--	--

	должны поставлять в виде встроенного специализированного агента в состав антивирусного решения разработчика и обеспечивать реализацию следующих функциональных возможностей: • совместимость агента с антивирусными решениями разработчика программного средства; Поддержку установки на 32-битных операционных систем следующих версий: - o Debian GNU/Linux 11.0 и выше. - o Debian GNU/Linux 12.0 и выше. - o Mageia 4. - o Альт 8 СП Рабочая Станция (8.4). - o Альт 8 СП Сервер (8.4). Поддержку установки на 64-битных операционных систем следующих версий: - o AlmaLinux OS 8 и выше. - o AlmaLinux OS 9 и выше. - o AlterOS 7.5 и выше. - o Amazon Linux 2. - o Astra Linux Common Edition 2.12. - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) - o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6). - o Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6). - o Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7). - o CentOS 7.2 и выше. - o CentOS Stream 8. - o CentOS Stream 9. - o Debian GNU/Linux 11.0 и выше. - o Debian GNU/Linux 12.0 и выше. - o EMIAS 1.0 и выше. - o EulerOS 2.0 SP10. - o Kylin 10. - o Linux Mint 21.1 и выше. - o Linux Mint 22.0 и выше. - o Mostech 12. - o openSUSE Leap 15.0 и выше. - o Oracle Linux 7.3 и выше. - o Oracle Linux 8.0 и выше. - o Oracle Linux 9.0 и выше. - o Red Hat Enterprise Linux 7.2 и выше. - o Red Hat Enterprise Linux 8.0 и выше. - o Red Hat Enterprise Linux 9.0 и выше.
--	---

	- o Rocky Linux 8.5 и выше. - o Rocky Linux 9.0 и выше. - o SberLinux 9.0.1. - o SberOS 3.3.3. - o SUSE Linux Enterprise Server 12.5 и выше. - o SUSE Linux Enterprise Server 15 и выше. - o Ubuntu 22.04 LTS. - o Ubuntu 24.04 LTS. - o Альт 8 СП Рабочая станция (8.4). - o Альт 8 СП Сервер (8.4). - o Альт Образование 10.1. - o Альт СП Рабочая Станция релиз 10. - o Альт СП Рабочая Станция релиз 10.1. - o Альт СП Сервер релиз 10. - o Альт СП Сервер релиз 10.1. - o Атлант, сборка Alcyone, версия 2022.02. - o Гослинукс 7.17. - o Гослинукс 7.2. - o М ОС 12 Сервер. - o МОС ОС 15.4 Арбат. - o МСВСФЕРА АРМ 9.2 и выше. - o МСВСФЕРА СЕРВЕР 9.2 и выше. - o ОС МЭШ 12 Для всех пользователей (без телеметрии и без поддержки ДИТ). - o ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ). - o ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ). - o Основа 2.9 и выше. - o РЕД ОС 7.3. - o РЕД ОС 8.0. - o РОСА "Кобальт" 7.9. - o РОСА "Хром" 12. - o СинтезМ-Клиент 8.6. - o СинтезМ-Сервер 8.6. Поддержку установки на 64-битные операционные системы для архитектуры ARM: - o Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7). - o CentOS Stream 9. - o EulerOS 2.0 SP10. - o SUSE Linux Enterprise Server 15. - o Ubuntu 22.04 LTS. - o Альт СП Рабочая Станция релиз 10. - o Альт СП Сервер релиз 10. - o РЕД ОС 7.3. - o РЕД ОС 8.0. • предоставлять расширенную информацию по новым обнаружениям от антивирусного решения разработчика программного средства в виде: - o графа цепочки развития угрозы;
--	--

	о информации об устройстве, на котором обнаружена угроза, включающей IP-адрес, MAC и версию ОС; о общей информации об обнаружении, включающей время обнаружения, имя объекта, параметры запуска объекта при их наличии, каталог нахождения объекта, его контрольные суммы MD5 и SHA256, имя учетной записи, режим обнаружения(например, обнаружение при сканировании по требованию или при автоматическом сканировании); о ссылки на веб-ресурс разработчика(Threat Intelligence) для просмотра расширенной информации по объекту обнаружения; о изменений в реестре, информации о созданных файлах, запущенных процессах, сетевых соединениях связанных с обнаружением; о принятых антивирусным решением разработчика программного средства ответных действий. • обеспечивать возможность реагирования на выявленные угрозы из карточки инцидента, на основе автоматизированного выполнения следующих задач и применение политик для искомого устройства либо сразу для группы устройств: - о изолировать устройство, на котором произошел алерт; - о поместить файл на карантин; - о создать задачу Поиска ИОС; - о запретить запуск обнаруженного файла; - о завершение процесса на устройстве; - о запуск процесса на устройстве; - о получение файла; - о удаление файла. • обеспечивать возможность реагирования на выявленные угрозы при обнаружении индикаторов компрометации(ИОС) для искомого устройства либо сразу для группы устройств: - о сетевая изоляция устройства; - о запускать проверку важных областей; - о копию поместить на карантин, объект удалить; • поддерживать возможность формирования индикаторов компрометации(ИОС) из обнаружения, сделанного антивирусным решением разработчика для последующего сканирования на устройствах на основе следующих объектов: - о описание файлов(контрольная сумма/расположение файла); - о пути и ключи реестра; • поддерживать экспорт и импорт индикаторов компрометации(ИОС) в формате
--	--

	OpenIOC; • детали обнаружения должны содержать информацию о группе доверия, цифровой подписи, данные о распространении файла • запуск файлов в облачной изолированной среде для выявления вредоносной активности и возможность включения отдельного счетчика для этой технологии. • наличие подсказок к функциям реагирования на угрозы. • наличие пошаговой инструкции по обеспечению безопасности инфраструктуры организации при обнаружении индикаторов компрометации • создавать специальную задачу для осуществления сканирования заданных областей на устройстве или группе устройств по заданным индикаторам компрометации(IOC) по расписанию или по требованию с возможностью просмотра результатов сканирования; • поддерживать все описанные сценарии работы с решением через веб-интерфейс средства централизованного управления Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: - о Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная. - о Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSC) 64-разрядная. - о Windows Server 2019 Standard/Datacenter/Core 64-разрядная. - о Windows Server 2022 Standard/Datacenter/Core 64-разрядная. - о Windows Storage Server 2019 64-разрядная. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: - о VMware vSphere 6.7. - о VMware vSphere 7.0. - о Microsoft Hyper-V Server 2019 64-разрядная. - о Microsoft Hyper-V Server 2022 64-разрядная. - о Citrix XenServer 7.1 LTSR. - о Citrix XenServer 8.x. - о Parallels Desktop 18. - о Oracle VM VirtualBox 7.x.
--	--

	Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: - о Microsoft SQL Server 2016 (все редакции) 64-разрядная. - о Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная. - о Microsoft SQL Server 2019 (все редакции) для Windows/Linux 64-разрядная (требуется дополнительные действия). - о Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная. - о MySQL 5.7 Community 32-разрядная/64-разрядная. - о MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная. - о MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная. - о MariaDB 10.5 (сборка 10.5.27 и выше) 32-разрядная/64-разрядная. - о MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB. - о PostgreSQL 13.x 64-разрядная. - о PostgreSQL 14.x 64-разрядная. - о PostgreSQL 15.x 64-разрядная. - о Postgres Pro 13.x Windows/Linux 64-разрядная. - о Postgres Pro 14.x Windows/Linux 64-разрядная. В программном средстве антивирусной защиты должны быть 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 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 карантинных 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; • возможность управления развертыванием ОС Windows через консоль управления; • наличие преднастроенных ролей пользователей средств централизованного управления; • должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей; • возможность подключения по RDP или штатными средствами из консоли управления; • наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing); • пользователю должен выводиться запрос на разрешение дистанционного подключения; • наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС; • возможность импортировать образ операционной системы из дистрибутивов (WIM) • наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии; • автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF • 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. • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; • возможность развернуть Сервер администрирования как систему высокой доступности; • возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети. • удаленная диагностика клиентских устройств на базе Windows и Linux (получение трассировок, журналов событий, дампов, остановка и запуск приложений); • возможность отозвать права локального администратора учетных записей на управляемых устройствах с операционной системой Linux; • возможность изменить пароль локальной учетной записи на управляемых устройствах с операционной системой Linux. Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: - о Debian GNU/Linux 11.x (Bullseye) 64-разрядная. - о Debian GNU/Linux 12 (Bookworm) 64-разрядная. - о Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная. - о Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная. - о CentOS Stream 9 64-разрядная. - о Red Hat Enterprise Linux Server 7.x 64-разрядная. - о Red Hat Enterprise Linux Server 8.x 64-разрядная. - о Red Hat Enterprise Linux Server 9.x 64-разрядная. - о SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная. - о SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная. - о Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
--	--

	- о Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная. - о Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная. - о Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная. - о Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная. - о Astra Linux Special Edition RUSB.10015-03 (обновление 7.6) 64-разрядная. - о Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная. - о Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная. - о Альт СП Сервер 10 64-разрядная. - о Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная. - о Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная. - о Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная. - о Альт СП Рабочая станция 10 64-разрядная. - о Oracle Linux 7 64-разрядная. - о Oracle Linux 8 64-разрядная. - о Oracle Linux 9 64-разрядная. - о Platform V SberLinux OS Server (SLO) 8.9.2 64-разрядная. - о РЕД ОС 7.3 Сервер 64-разрядная. - о РЕД ОС 7.3 Сертифицированная редакция 64-разрядная. - о РЕД ОС 8 64-разрядная. - о РОСА "КОБАЛЬТ" 7.9 64-разрядная. - о М ОС (Moscow Electronic School) 12 Сервер 64-разрядная. - о Mostech Server 64-разрядная. - о МосОС 15.4 Arbat 64-разрядная. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: - о VMware vSphere 6.7.0. - о VMware vSphere 7.0.3. - о Microsoft Hyper-V Server 2019 64-разрядная. - о Microsoft Hyper-V Server 2022 64-разрядная. - о Citrix XenServer 7.x. - о Citrix XenServer 8.2. - о Parallels Desktop 18. - о Oracle VM VirtualBox 7.0.12. - о Kernel-based Virtual Machine (все поддерживаемые ОС Linux). Программные средства централизованного управления, мониторинга и обновления должны
--	--

	функционировать с СУБД следующих версий: - о MySQL 5.7 Community 32-разрядная/64-разрядная. - о MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная. - о MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная. - о MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная. - о MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная. - о MariaDB 10.4 (сборка 10.4.20 и выше) 32-разрядная/64-разрядная. - о MariaDB 10.5 (сборка 10.5.27 и выше) 32-разрядная/64-разрядная. - о MariaDB 10.6 (сборка 10.6.20 и выше) 32-разрядная/64-разрядная. - о MariaDB 10.11 (сборка 10.11.10 и выше) 32-разрядная/64-разрядная. - о MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB. - о PostgreSQL 13.x 64-разрядная. - о PostgreSQL 14.x 64-разрядная. - о PostgreSQL 15.x 64-разрядная. - о PostgreSQL 15.x 64-разрядная (кластер Corosync/Pacemaker). - о PostgreSQL 16.x 64-разрядная. - о PostgreSQL 17 64-разрядная. - о Postgres Pro 13.x (все редакции) 64-разрядная. - о Postgres Pro 14.x (все редакции) 64-разрядная. - о Postgres Pro 15.x (все редакции) 64-разрядная. - о Postgres Pro 15.x 64-разрядная (кластер Corosync/Pacemaker). - о Postgres Pro 16.x (все редакции) 64-разрядная. - о Postgres Pro 16.x Enterprise 64-разрядная (кластер Built-in High Availability). - о Postgres Pro 17 (все редакции) 64-разрядная. - о Postgres Pro 17 Enterprise 64-разрядная (кластер Built-in High Availability). - о Platform V Pangolin 5.4.0 64-разрядная. - о Jatoba 4 64-разрядная. В программном средстве антивирусной защиты должны быть 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 карантин 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; • выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных; • экспорт и импорт выборок событий; • получение информации о программах, установленных на управляемые устройства; • возможность поиска устройств по контроллерам доменов Microsoft Active Directory и Samba; • возможность автоматизированного переноса данных с сервера администрирования под управлением ОС Windows на сервер администрирования под управлением ОС Linux; • возможность удалённой диагностики управляемых устройств; • поддержка кластерной технологии; • возможность централизованного удаления несовместимого ПО с управляемых устройств. Требования к обновлению антивирусных баз Обновляемые антивирусные базы данных должны обеспечивать 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
--	--

	Обновляемые антивирусные базы данных должны обеспечивать 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 • 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 Республики Казахстан по электронной почте и через Интернет. • Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов. • Поставщик проведет инструктаж вводного курса поставляемого программного продукта. Вводный курс будет закреплён практическими занятиями, с предоставлением электронных методических пособий. По окончании вводного курса Поставщик обеспечит слушателям выдачу сертификата. Вводный курс будет проведён в течение месяца после заключения договора. • В рамках услуги Поставщик выполнить установку антивирусного программного обеспечения и соответствующих компонентов защиты; • проверить корректность работы основных компонентов защиты после установки;
--	--

Руководитель департамента
цифровой трансформации и развития систем



А. Хамитжан

Бағдарламалық қамтамасыз етуді пайдалану құқығына берілетін лицензиялардың қолданылу мерзімін ұзарту бойынша сатып алынатын қызметтердің техникалық ерекшелігі

Тауарлардың, жұмыстардың және көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*	582950.000.000000
Қызметтің атауы*	Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер
Өлшем бірлігі*	Бір қызмет
Саны (көлемі)*	1
Қызмет көрсету мерзімі*	Тапсырыс беруші өтінім берген күннен бастап 16 күнтізбелік күн ішінде
Кепілдік мерзімі (айлармен)	Кемінде 12
Қажетті сипаттамалардың, параметрлердің және басқа да бастапқы деректердің сипаттамасы:	Сатып алу мақсаты: 250 құрылғыға арналған Kaspersky Security for Business EDR Оптимальный антивирустық бағдарламалық қамтамасыз етуді пайдалану құқығына берілген қолданыстағы лицензияның қолданылу мерзімін 12 айға ұзарту Жалпы талаптар Антивирустық құралдар мыналарды қамтуы тиіс: » Windows жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары; » MacOS жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары; » Linux жұмыс станциялары мен серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдары; » Windows файлдық серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдары; » мобильді құрылғыларға (смартфондар мен планшеттерге) арналған антивирустық қорғаудың бағдарламалық құралдары; » орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары; » зиянды бағдарламалар мен шабуылдардың жаңартылатын сигнатуралық дерекқорлары; » орыс тіліндегі пайдалану құжаттамасы. Басқару құралдарын қоса алғанда, барлық антивирустық құралдардың бағдарламалық интерфейсі орыс және ағылшын тілдерінде болуы тиіс. Басқару құралдарын қоса алғанда, барлық антивирустық құралдарда орыс және ағылшын тілдеріндегі контекстік анықтамалық жүйе болуы тиіс.

	разрядты); - o Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise/Enterprise multi-session; - o Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • нақты уақыт режимінде және объектінің контекстік мәзірінен сұрау бойынша антивирустық сканерлеу; • антивирустық сканерлеуді кесте бойынша орындау; • қосылатын құрылғыларды антивирустық сканерлеу; • бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; • белсенді жұқтыру әрекеттерін залалсыздандыру; • зиянды белсенділікті анықтау және рұқсат етілмеген әрекеттерді айқындау мақсатында қолданбаның мінез-құлқын және оның жүйеде орындайтын әрекеттерін талдау; • желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау мақсатында ортақ бумалар мен файлдарға жасалатын қатынауларды талдау; • бағдарламалық қамтамасыз етудегі осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестердің жадын қорғау; • емдеу кезінде зиянды бағдарламалық қамтамасыз етудің әрекеттерін кері қайтару, оның ішінде зиянды бағдарламалар шифрлаған файлдарды қалпына келтіру; • процестер мен қолданбалар үшін артықшылықтарды шектеу (тізілімге жазу, файлдарға, бумаларға және басқа процестерге қол жеткізу, тапсырмаларды жоспарлаушыға жүгіну, құрылғыларға қол жеткізу, объектілерге құқықтарды өзгерту және т.б.), сенім деңгейін анықтай отырып, қолданбалардың динамикалық түрде жаңартылатын теңшелетін тізімдері; • жаңа қауіптерден бұлттық қорғау, қолданбаға іске қосылатын бағдарлама немесе файл бойынша вердикт алу үшін нақты уақыт режимінде өндірушінің ресурстарына жүгінуге мүмкіндік беру; • RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматтарындағы архивтердегі файлдарды антивирустық тексеру және емдеу; • электрондық поштаны зиянды
--	---

	бағдарламалардан қорғау, IMAP, SMTP, POP3, MAPI, NNTP хаттамалары бойынша берілетін кіріс және шығыс трафикті тексеру; • файлдардың белгіленген түрлерін қайта атау немесе жою мүмкіндігі бар пошта тіркемелерінің сүзгісі; • HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP хаттамалары бойынша пайдаланушы компьютеріне келіп түсетін желілік трафикті, оның ішінде эвристикалық талдау көмегімен тексеру, сенімді ресурстарды теңшеу және бұғаттау немесе статистика режимінде жұмыс істеу мүмкіндігі; • жүктелетін Web-беттердегі баннерлер мен қалқымалы терезелерді бұғаттау; • фишингтік және қауіпті сайттарды тану және бұғаттау; • желілік пакет ережелерін және бағдарламаларға арналған желілік ережелерді жасауға мүмкіндік беретін, желілік сегменттерді санаттау мүмкіндігі бар кіріктірілген желілік экран; • кез келген типтегі есептеу желілерінде қолданбалар мен порттарға арналған желілік экран ережелерін пайдалана отырып, желілік шабуылдардан қорғау; • құрылғының MAC-мекенжайын қолдан жасау үшін ARP хаттамасындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау; • желілік көпір типіндегі желілік қосылымдарды бақылау, бірнеше желілік қосылымды бір уақытта орнатуды бұғаттау мүмкіндігі; • барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді жасау, компонент қолданбаларды бағдарламаның орналасу жолы, метадеректері, сертификаты немесе оның отпечатогы, бақылау сомасы бойынша, сондай-ақ бағдарламалық қамтамасыз ету өндірушісі ұсынатын алдын ала белгіленген қолданбалар санаттары бойынша бақылауы тиіс, компонент қара немесе ақ тізім режимінде, сондай-ақ статистика жинау немесе бұғаттау режимінде жұмыс істеуі тиіс; • сыртқы енгізу/шығару құрылғыларымен жұмыс істеуді құрылғы түрі және/немесе пайдаланылатын шина бойынша бақылау, олардың идентификаторы бойынша сенімді құрылғылар тізімін жасау мүмкіндігі және Active Directory жүйесінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалануға
--	--

	артықшылықтар беру мүмкіндігі; • құрылғыларды бақылау шеңберінде МТР құрылғыларын басқару және осы типтегі құрылғыларға барлық немесе пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін қол жеткізу ережелерін теңшеу; • алынбалы дискілерге файлдарды жазу және/немесе олардан файлдарды жою туралы оқиғалар журналына жазу; • файлдық жүйесі бар құрылғыларға қол жеткізу ережелерінің басымдығын тағайындау; • пайдаланушының Интернет желісімен жұмыс істеуін бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға қол жеткізуге нақты тыйым салуды немесе рұқсат беруді қосу, өндіруші жасаған және динамикалық түрде жаңартылатын санаттарға, сондай-ақ ақпарат түріне (аудио, видео және т.б.) қол жеткізуді басқару уақыт аралықтарын енгізу, сондай-ақ оны тек Active Directory жүйесіндегі белгілі бір пайдаланушыларға тағайындау; • BadUSB типіндегі шабуылдардан қорғау; • қолданба сервисін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ қолданба параметрлеріне пароль арқылы қол жеткізуді қорғау; • параметрлерді сенімді қашықтан әкімшілендіру бағдарламалары арқылы басқару; • антивирустық қорғау бағдарламалық құралының тек таңдалған компоненттерін орнату; • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару; • тапсырмаларды кесте бойынша және/немесе қолданба іске қосылғаннан кейін бірден іске қосу; • файлдық кеңістікті сканерлеу кезінде пайдаланушылардың жайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару; • алдыңғы тексеруден кейінгі күйі өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету; • антивирустық бағдарламаның тұтастығын тексеру; • файлдың бақылау сомасы, атау/каталог маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу; • ережелер мен ерекшеліктер тізімдерін XML-форматына импорттау және экспорттау; • антивируста жойылған вирус жұққан
--	--

	файлдарға арналған қорғалған қойманың болуы, оларды қалпына келтіру мүмкіндігі; • антивирустың жұмысы туралы есептерге арналған қорғалған қойманың болуы; • антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктерінің ең аз жиынтығы бар графикалық интерфейсін жеңілдетілген нұсқасының болуы; • Windows Defender Security Center жүйесімен интеграция; • Antimalware Scan Interface (AMSI) қолдауының болуы; • Windows Subsystem for Linux (WSL) қолдауының болуы; • резервтік қоймадан объектілерді қалпына келтіруді парольмен қорғау; • Интернетке қосылу лимиттелген болған жағдайда желілік трафикті шектеу; • TCP және UDP хаттамалары бойынша желіні мониторингтеу құралының болуы; • тексеру тапсырмасын қайта жүктегеннен кейін тексеру үзілген жерден жалғастыру; • тапсырманың орындалу ұзақтығына шектеу орнату; • тексеру орындалып жатқан жағдайда тексеру тапсырмаларын кезекке қою мүмкіндігі; • жұмыс станциясының желілік көпірлердің құрылуына жол бермеу мақсатында ақпарат берудің әртүрлі арналары (сымды және сымсыз) бойынша желілік қосылымдарды бір уақытта орнатуына тыйым салуға арналған Анти-Бриджинг функциясының болуы; • жүйені қайта жүктемей жаңарту; • портативті құрылғылар (MTP) үшін қол жеткізу құқықтарын (оқу / жазу) теңшеу, құрылғыларға қол жеткізе алатын пайдаланушыларды немесе пайдаланушылар тобын таңдау, сондай-ақ құрылғыларға қол жеткізу кестесін белгілеу; • Android Debug Bridge (ADB) қолданбасында пайдаланушылардың мобильді құрылғыларға қол жеткізуін теңшеу; • мобильді құрылғыға қол жеткізуге тыйым салынған жағдайда да құрылғыны компьютерге USB арқылы қосу арқылы мобильді құрылғыны зарядтау; • пайдаланушылар үшін басып шығару құқықтарын теңшеу; • Wi-Fi желілеріне қосылуды бақылау үшін WPA3 хаттамасын қолдаудың болуы; • Azure WVD-мен үйлесімділіктің болуы; • iTunes қолданбасында пайдаланушылардың мобильді құрылғыларға қол жеткізуін теңшеу; • компьютерде орнатылған қолданбалардағы осалдықтарды анықтау және жою үшін арнайы
--	---

	тапсырманы іске қосу, анықталған осалдықтар бойынша есеп ұсыну мүмкіндігі; • арнайы жүктеу агентін құрумен және Single Sign On технологиясын қолдаумен толық дискілік шифрлау, UEFI жүйелерін қолдау; • жүктеу агенті немесе ОС файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI жүйелерін қолдау; • толық дискілік шифрлау кезінде екі факторлы аутентификацияны қолдау; • шифрланатын мазмұнды икемді көрсету мүмкіндігімен файлдарды шифрлау (орналасқан жері, кеңейтімі, файлды жасайтын қолданба бойынша); • таңдалған қолданбалар тарапынан шифрланған файлдарға қол жеткізуді шектеу механизмдерінің болуы, сондай-ақ ұйымнан тыс жерде файлдарды пароль арқылы шифрлаудан шығару технологиясының болуы; • алынбалы тасымалдағыштардағы деректерді шифрлау, ұйым желісінен тыс жерде файлдарды шифрлауға және шифрлаудан шығаруға мүмкіндік беретін жұмыс режимін орнату мүмкіндігі; • бағдарламалардың мінез-құлық үлгісін қалыптастыру және мінез-құлық үлгісінен ауытқыған кезде олардың әрекеттерін бұғаттау мүмкіндігі (аномалияларды бейімделмелі бақылау); • дискіні шифрлау кезінде аутентификация агентінің қызметтік есептік жазбасын жасау мүмкіндігі; • толық дискілік шифрлау кезінде SSO жұмысына арналған ADSelfService Plus үшінші тарап есептік деректер провайдерін қолдау; • енгізу құрылғыларынан басқа барлық Bluetooth-құрылғыларға арналған ерекшеліктерді теңшеу және оларға қол жеткізуді шектеу мүмкіндігі; • операциялық жүйені қайта жүктемей қолданбаны жаңарту мүмкіндігі; • зиянды бағдарламаларды іздеу тапсырмасы үшін процессор ресурстарын тұтынуды шектеу мүмкіндігі; • қолданба қызметтерін сырттан басқаруға тыйым салу мүмкіндігі. Windows серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдарына қойылатын талаптар Антивирустық қорғаудың бағдарламалық құралдары файлдық серверлерге арналған операциялық жүйелердің мынадай нұсқаларын басқаратын компьютерлерде жұмыс істейтін: - o Windows Small Business Server 2011 Essentials / Standard (64-разрядты), Microsoft Small Business Server 2011 Standard (64-разрядты) мек Microsoft
--	---

	Windows Server 2008 R2 үшін Service Pack 1 орнатылған кезде қолдау көрсетіледі; - o Windows MultiPoint Server 2011 (64-разрядты); - o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 және одан жоғары; - o Windows Server 2012 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2016 Essentials / Standard / Datacenter; - o Windows Server 2019 Essentials / Standard / Datacenter; - o Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Core Mode қоса алғанда) Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • нақты уақыт режимінде және объектінің контекстік мәзірінен сұрау бойынша антивирустық сканерлеу; • антивирустық сканерлеуді кесте бойынша орындау; • қосылатын құрылғыларды антивирустық сканерлеу; • бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; • белсенді жұқтыру әрекеттерін залалсыздандыру; • зиянды белсенділікті анықтау және рұқсат етілмеген әрекеттерді айқындау мақсатында қолданбаның мінез-құлқын және оның жүйеде орындайтын әрекеттерін талдау; • желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау мақсатында ортақ бумалар мен файлдарға жасалатын қатынауларды талдау; • бағдарламалық қамтамасыз етудегі осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестердің жадын қорғау; • емдеу кезінде зиянды бағдарламалық қамтамасыз етудің әрекеттерін кері қайтару, оның ішінде зиянды бағдарламалар шифрлаған файлдарды қалпына келтіру; • жаңа қауіптерден бұлттық қорғау, қолданбаға іске қосылатын бағдарлама немесе файл бойынша вердикт алу үшін нақты уақыт режимінде өндірушінің ресурстарына жүгінуге мүмкіндік беру; • RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматтарындағы архивтердегі файлдарды
--	--

	антивирустық тексеру және емдеу; • желілік пакет ережелерін және бағдарламаларға арналған желілік ережелерді жасауға мүмкіндік беретін, желілік сегменттерді санаттау мүмкіндігі бар кіріктірілген желілік экран; • құрылғының MAC-мекенжайын қолдан жасау үшін ARP хаттамасындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау; • қолданба сервисін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалар, қаскүнемдер немесе біліктілігі жоқ пайдаланушылар тарапынан қорғауды өшіруге жол бермеуге мүмкіндік беретін қолданба параметрлеріне пароль арқылы қол жеткізуді қорғау; • антивирустық қорғау бағдарламалық құралының тек таңдалған компоненттерін орнату; • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару; • тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; • файлдық кеңістікті сканерлеу кезінде пайдаланушылардың жайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару; • алдыңғы тексеруден кейінгі күйі өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету; • антивирустық бағдарламаның тұтастығын тексеру; • файлдың бақылау сомасы, атау/каталог маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу; • антивируста жойылған вирус жұққан файлдарға арналған қорғалған қойманың болуы, оларды қалпына келтіру мүмкіндігі; • антивирустың жұмысы туралы есептерге арналған қорғалған қойманың болуы; • антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктерінің ең аз жиынтығы бар графикалық интерфейсін жеңілдетілген нұсқасының болуы; • Windows Defender Security Center жүйесімен интеграция; • Antimalware Scan Interface (AMSI) қолдауының болуы; • Windows Subsystem for Linux (WSL) қолдауының болуы; • резервтік қоймадан объектілерді қалпына
--	---

	келтіруді парольмен қорғау. • ережелер мен ерекшеліктер тізімдерін XML-форматына импорттау және экспорттау; • Интернетке қосылу лимиттелген болған жағдайда желілік трафикті шектеу; • барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді жасау, компонент қолданбаларды бағдарламаның орналасу жолы, метадеректері, сертификаты немесе оның отпечатоғы, бақылау сомасы бойынша, сондай-ақ бағдарламалық қамтамасыз ету өндірушісі ұсынатын алдын ала белгіленген қолданбалар санаттары бойынша бақылауы тиіс, компонент қара немесе ақ тізім режимінде, сондай-ақ статистика жинау немесе бұғаттау режимінде жұмыс істеуі тиіс; • компьютерде орнатылған қолданбалардағы осалдықтарды анықтау және жою үшін арнайы тапсырманы іске қосу, анықталған осалдықтар бойынша есеп ұсыну мүмкіндігі; • Windows серверлеріне арналған операциялық жүйемен жұмыс істейтін компьютерлер үшін Веб-қауіптерден қорғау, Пошта қауіптерінен қорғау, Веб-бақылау және Құрылғыларды бақылау компоненттерін қолдау; • тексеру тапсырмасын қайта жүктегеннен кейін тексеру үзілген жерден жалғастыру; • тапсырманың орындалу ұзақтығына шектеу орнату мүмкіндігі; • тексеру орындалып жатқан жағдайда тексеру тапсырмаларын кезекке қою мүмкіндігі; • жүйені қайта жүктемей жаңарту; • портативті құрылғылар (МТР) үшін қол жеткізу құқықтарын (оқу / жазу) теңшеу, құрылғыларға қол жеткізе алатын пайдаланушыларды немесе пайдаланушылар тобын таңдау, сондай-ақ құрылғыларға қол жеткізу кестесін белгілеу; • мобильді құрылғыға қол жеткізуге тыйым салынған жағдайда да құрылғыны компьютерге USB арқылы қосу арқылы мобильді құрылғыны зарядтау; • пайдаланушылар үшін басып шығару құқықтарын теңшеу; • Wi-Fi желілеріне қосылуды бақылау үшін WPA3 хаттамасын қолдаудың болуы; • Azure WVD-мен үйлесімділіктің болуы; • операциялық жүйені қайта жүктемей қолданбаны жаңарту мүмкіндігі; • зиянды бағдарламаларды іздеу тапсырмасы үшін процессор ресурстарын тұтынуды шектеу
--	---

	мүмкіндігі. • қолданба қызметтерін сырттан басқаруға тыйым салу мүмкіндігі. • SQL-серверлерде, Microsoft Exchange-серверлерінде және System Center Configuration Manager-де қолданбаның жұмысы үшін сенімді аймақты жылдам теңшеуге арналған тексеруден алдын ала орнатылған ерекшеліктер мен сенімді қолданбаларды пайдалану мүмкіндігі. Мас жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдарына қойылатын талаптар Мас жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары мынадай нұсқалардағы операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі тиіс: о macOS 11 - 15; Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • резиденттік антивирустық мониторинг; • жаңа қауіптерден бұлттық қорғау, қолданбаға іске қосылатын бағдарлама немесе файл бойынша вердикт алу үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беру; • антивирустық базаларды кесте бойынша автоматты түрде жаңарту; • вирус жұққан файлдарды жою алдында қалпына келтіру мүмкіндігі үшін олардың резервтік көшірмесін жасау; • бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; • IDS/IPS шабуылдарды анықтау және алдын алу жүйесін және сымсыз желілерді қоса алғанда, кез келген типтегі есептеу желілерінде жұмыс істеген кезде ең танымал қолданбалар үшін желілік белсенділік ережелерін пайдалана отырып, желілік шабуылдардан қорғау; • антивирустық қорғау құралдарын өндірушінің бұлттық репутациялық сервистерінің вердикттері негізінде зиянды және фишингтік сайттарды бұғаттау; • Safari, Google Chrome және Firefox браузерлері арқылы берілетін желілік трафикті (HTTP және HTTPS трафигі) тексеру; • пайдаланушының Интернет желісімен жұмыс істеуін бақылау, оның ішінде санаттарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартылатын белгілі бір ресурстарға немесе ресурстар санаттарына қол жеткізуге нақты тыйым салуды немесе рұқсат беруді қосу;
--	--

	• алдыңғы тексеруден кейінгі күйі өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету; • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару; • FileVault шифрлауын басқару мүмкіндігімен жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару; • көрсетілген аймақтарды файлдық операцияларды ұстап қалу деңгейінде тексеру кезінде ерекшеліктерді белгілеу мүмкіндігі; • дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілген бойда қажетті жүйелік кеңейтімдерді орнату мүмкіндігі; • зиянды бағдарламаларды іздеу тапсырмаларын орындау кезінде қолданба арқылы процессордың жүктелуін шектеу; • операциялық жүйе ресурстарына түсетін жүктемені азайту үшін бұлттық режимді қосу және зиянды бағдарламалар базаларының жеңілдетілген нұсқасын пайдалану; • сұрау бойынша тексеру тапсырмаларын орындау кезінде тек оқуға қолжетімді жүйелік томды сканерлеуді өткізіп жіберу; • BSS қауіпті мінез-құлық үлгілерін пайдалана отырып, операциялық жүйедегі қолданбалардың белсенділігін талдау; • JAMF арқылы .pkg файлынан орнату; • сыртқы дискілерді қосқан кезде оларды автоматты түрде сканерлеу; • клиенттік сертификаттарды қолдау. Linux жұмыс станциялары мен серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдарына қойылатын талаптар Linux жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары келесі нұсқалардағы 32-биттік операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі тиіс: - o Debian GNU/Linux 11.0 және одан жоғары. - o Debian GNU/Linux 12.0 және одан жоғары. - o Mageia 4. - o Альт 8 СП Рабочая Станция (8.4). - o Альт 8 СП Сервер (8.4). - o Альт Образование 10. - o Альт Рабочая Станция 10. Linux жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары келесі нұсқалардағы 64-биттік операциялық жүйелерді басқаратын
--	--

	компьютерлерде жұмыс істеуі тиіс: - o AlmaLinux OS 8 және одан жоғары. - o AlmaLinux OS 9 және одан жоғары. - o AlterOS 7.5 және одан жоғары. - o Amazon Linux 2. - o Astra Linux Common Edition 2.12. - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7). - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) - o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6). - o Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6). - o Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7). - o CentOS 7.2 және одан жоғары. - o CentOS Stream 8. - o CentOS Stream 9. - o Debian GNU/Linux 11.0 және одан жоғары. - o Debian GNU/Linux 12.0 және одан жоғары. - o EMIAS 1.0 және одан жоғары. - o EulerOS 2.0 SP10. - o Kylin 10. - o Linux Mint 20.3 және одан жоғары. - o Linux Mint 21.1 және одан жоғары. - o openSUSE Leap 15.0 және одан жоғары. - o Oracle Linux 7.3 және одан жоғары. - o Oracle Linux 8.0 және одан жоғары. - o Oracle Linux 9.0 және одан жоғары. - o Red Hat Enterprise Linux 7.2 және одан жоғары. - o Red Hat Enterprise Linux 8.0 және одан жоғары. - o Red Hat Enterprise Linux 9.0 және одан жоғары. - o Rocky Linux 8.5 және одан жоғары. - o Rocky Linux 9.1. - o SberLinux 8.8 (Dykhtau). - o SberLinux 8.9. - o SberOS 3.2.0. - o SUSE Linux Enterprise Server 12.5 және одан жоғары. - o SUSE Linux Enterprise Server 15 және одан жоғары. - o Ubuntu 20.04 LTS. - o Ubuntu 22.04 LTS. - o Ubuntu 24.04 LTS. - o Альт 8 СП Рабочая станция (8.4). - o Альт 8 СП Сервер (8.4). - o Альт Образование 10.1. - o Альт Рабочая Станция 10.1. - o Альт Сервер 10.1. - o Альт СП Рабочая Станция релиз 10.
--	---

	о Альт СП Сервер релиз 10. о Атлант, сборка Alcyone, версия 2022.02. о Гослинукс 7.17. о Гослинукс 7.2. о МСВСФЕРА АРМ 9.2 және одан жоғары. о МСВСФЕРА СЕРВЕР 9.2 және одан жоғары. о РЕД ОС 7.3. о РЕД ОС 8.0. о РОСА "Кобальт" 7.9. о РОСА "Хром" 12. о СинтезМ-Клиент 8.6. о СинтезМ-Сервер 8.6. АРМ архитектурасына арналған қолдау көрсетілетін 64-биттік операциялық жүйелер: о Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7). о CentOS Stream 9. о EulerOS 2.0 SP10. о SUSE Linux Enterprise Server 15. о Ubuntu 22.04 LTS. о Альт 8 СП Рабочая Станция (8.4). о Альт 8 СП Сервер (8.4). о Альт СП Рабочая Станция релиз 10. о Альт СП Сервер релиз 10. о РЕД ОС 7.3. о РЕД ОС 8.0. Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • резиденттік антивирустық мониторинг; • жаңа қауіптерден бұлттық қорғау, қолданбаға іске қосылатын бағдарлама немесе файл бойынша вердикт алу үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беру; • SMB / NFS арқылы қолжетімді ресурстарды тексеру; • ядро жадын тексеру мүмкіндігі; • бұрын белгісіз зиянды бағдарламаларды неғұрлым тиімді тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; • пайдаланушының немесе әкімшінің командасы бойынша және кесте бойынша антивирустық сканерлеу; • zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; bz2; .tbz; .tbz2; .gz; .tgz; .arj. архивтеріндегі файлдарды антивирустық тексеру; • электрондық пошта хабарламаларын мәтіндік форматта (Plain text) тексеру; • файлдарды тексеруді оңтайландыру механизмдерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытын шектеу, тексерілетін файл өлшемін шектеу, тексерілген және тексеруден кейін өзгермеген файлдар
--	--

	туралы ақпаратты кәштеу механизмі); • SMB / NFS хаттамалары бойынша желілік қолжетімділігі бар жергілікті каталогтардағы файлдарды қашықтан зиянды шифрлаудан қорғау; • тексеру кезінде файлдарды бұғаттау опциясын қосу; • күдікті және бүлінген объектілерді карантинге орналастыру; • SAMBA деңгейінде файлдық операцияларды ұстап қалу және тексеру; • операциялық жүйенің желілік экранын басқару, ережелердің бастапқы күйін қалпына келтіру мүмкіндігі; • тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; • есептерді HTML және CSV форматтарында экспорттау және сақтау; • файлдық кеңістікті сканерлеу кезінде пайдаланушылардың жайлы жұмысын қамтамасыз ету үшін ДК ресурстарын пайдалануды икемді басқару; • объектінің ақпараттық құндылығы болған жағдайда сұрау бойынша қалпына келтіру мүмкіндігі мақсатында емдеу және жою алдында вирус жұққан объектінің көшірмесін резервтік қоймада сақтау; • root құқықтарынсыз пайдаланушының графикалық интерфейсі арқылы басқару; • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі немесе веб-консоль арқылы орталықтандырылған басқару; • пайдаланушылардың компьютерге орнатылған немесе қосылған құрылғыларға қол жеткізуін құрылғы түрлері және қосылу шиналары бойынша басқару; • алынбалы дискілерді тексеру; • кіріс желілік трафикте желілік шабуылдарға тән белсенділікті бақылау; • HTTP/HTTPS және FTP хаттамалары бойынша пайдаланушы компьютеріне түсетін трафикті тексеру, сондай-ақ веб-мекенжайлардың зиянды немесе фишингтік екенін анықтау мүмкіндігі; • пайдаланушы компьютеріндегі бағдарламалардың әрекеттері туралы деректерді алу; • компьютерлерде сақталған бағдарламалардың барлық орындалатын файлдары туралы ақпаратты алу (Инвентаризация тапсырмасы); • бағдарламаны іске қосу кезінде трассировка файлдарын жасау; • компьютерлерде орнатылған бағдарламалардың барлық орындалатын
--	---

	файлдары туралы ақпарат алу; • автоматты іске қосу объектілерін, жүктеу секторларын, процестер жадын және ядро жадын тексеру; • емдеу немесе жою алдында файлдардың резервтік көшірмелерін сақтау және резервтік көшірмелерден файлдарды қалпына келтіру; • бағдарламаның жалпы параметрлерінде процестер жадын тексеруден процестерді алып тастау; • SkipPlainTextFiles параметрі арқылы бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру; • трафикті бағдарлама арқылы тексеруден алып тастау; • сұраулар мен ақпаратты шығару үшін, сондай-ақ бағдарламаның параметрлері мен тапсырмалардың параметрлерін экспорттау және импорттау үшін JSON форматын пайдалану; • Архитектурасына арналған операциялық жүйелері бар құрылғыларда орнату және жұмыс істеу; • қауіптер анықталған жағдайда немесе құрылғыға қол жеткізу әрекеті анықталған жағдайда пайдаланушыны хабардар ету режимінде жұмыс істеу; • тыйым салынған немесе рұқсат етілген қолданбалар тізімі режимдеріндегі бақылау ережелері арқылы қорғалатын құрылғыларда қолданбалардың іске қосылуын басқару мүмкіндігі; • жаңарту кезінде қолданбаны автоматты түрде қайта іске қосу; • процессор ресурстарын пайдалануға шектеу қою мүмкіндігі; • орнатудан кейін қолданбаны іске қосу кезінде қорғау компоненттері мен тексеру тапсырмаларын автоматты режимде өшіру мүмкіндігі; • графикалық пайдаланушы интерфейсінде компоненттер мен тапсырмалардың жұмысы туралы пайдаланушыға хабарламалар; • оларды тоқтатпай-ақ процестердің жадын оқу мүмкіндігі (3.4 нұсқасынан бастап Linux ядролары); • пайдаланушылардың веб-ресурстарға қол жеткізуін басқару мүмкіндігі; • қолданбаның өзіндік жұмысының тұрақтылығын мониторингтеу функциясы. Windows файлдық серверлеріне, кәсіпорын ауқымындағы серверлерге, Windows терминалдық серверлеріне арналған антивирустық қорғаудың бағдарламалық
--	---

	құралдарына қойылатын талаптар Windows файлдық серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдары мынадай нұсқалардағы операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі тиіс: Microsoft Windows 32-разрядты операциялық жүйелері - o Windows Server 2003 Standard / Enterprise / Datacenter Service Pack SP2 немесе одан жоғары жаңарту пакетімен; - o Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack SP2 немесе одан жоғары жаңарту пакетімен; - o Windows Server 2008 Standard / Enterprise / Datacenter Service Pack SP2 немесе одан жоғары жаңарту пакетімен; - o Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack SP2 немесе одан жоғары жаңарту пакетімен. Microsoft Windows 64-разрядты операциялық жүйелері - o Windows Server 2003 Standard / Enterprise / Datacenter Service Pack SP2 немесе одан жоғары жаңарту пакетімен; - o Windows Server 2003 R2 Standard / Enterprise / Datacenter Service Pack SP2 немесе одан жоғары жаңарту пакетімен; - o Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack SP2 немесе одан жоғары жаңарту пакетімен; - o Windows Server 2008 Standard / Enterprise / Datacenter Service Pack SP2 немесе одан жоғары жаңарту пакетімен; - o Microsoft Small Business Server 2008 Standard / Premium SP2 немесе одан жоғары; - o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack SP1 немесе одан жоғары жаңарту пакетімен; - o Windows Server 2008 R2 Core Standard / Enterprise / Datacenter Service Pack SP1 немесе одан жоғары жаңарту пакетімен; - o Windows Hyper-V Server 2008 R2 Service Pack SP1 немесе одан жоғары жаңарту пакетімен; - o Microsoft Small Business Server 2011 Essentials / Standard SP1 немесе одан жоғары; - o Microsoft Windows MultiPoint Server 2011 Standard / Premium; - o Windows Server 2012 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter; - o Microsoft MultiPoint Server 2012 Standard / Premium;
--	---

	- o Windows Storage Server 2012; - o Windows Hyper-V Server 2012; - o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; - o Windows Storage Server 2012 R2; - o Windows Hyper-V Server 2012 R2; - o Windows Server 2016 Essentials / Standard / Datacenter; - o Windows Server 2016 MultiPoint; - o Windows Server 2016 Core Standard / Datacenter; - o Microsoft Windows MultiPoint Server 2016; - o Windows Storage Server 2016; - o Windows Hyper-V Server 2016; - o Windows Server 2019 Essentials / Standard / Datacenter; - o Windows Server 2019 Core; - o Windows Storage Server 2019; - o Windows Hyper-V Server 2019; - o Windows Server 2022; - o Windows 10 Enterprise multi-session. Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • әртүрлі функцияларды орындайтын серверлерде: терминалдық серверлерде, басып шығару серверлерінде, қолданбалар серверлерінде және домен контроллерлерінде, файлдық серверлерде нақты уақыт режимінде және сұрау бойынша антивирустық сканерлеу; • пайдаланушының немесе әкімшінің командасы бойынша және кесте бойынша антивирустық сканерлеу; • тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; • жаңа қауіптерден бұлттық қорғау, қолданбаға іске қосылатын бағдарлама немесе файл бойынша вердикт алу үшін нақты уақыт режимінде өндірушінің арнайы сайттарына жүгінуге мүмкіндік беру; • RAR, ARJ, ZIP, CAB форматтарындағы архивтердегі файлдарды антивирустық тексеру және емдеу; • файлдарды, файлдық жүйелердің балама ағындарын (NTFS-streams), жүктеу жазбасын, жергілікті және алынбалы дискілердің жүктеу секторларын қорғау; • қорғалатын серверде Microsoft Windows Script Technologies (немесе Active Scripting) технологиялары бойынша жасалған VBScript және JScript скрипттерін орындау әрекеттерін үздіксіз бақылау, скрипттердің бағдарламалық кодын
--	--

	тексеру және қауіпті деп танылған скрипттердің орындалуына автоматты түрде тыйым салу; • желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау мақсатында ортақ бумалар мен файлдарға жасалатын қатынауларды талдау; • Microsoft Windows контейнерлерін тексеру; • процестер жадындағы осалдықтарды пайдаланудан қорғау; • бұзылған процестерді автоматты түрде аяқтау мүмкіндігі болуы тиіс, бұл ретте маңызды жүйелік процестер аяқталмауы тиіс; • процестерді қорғалатын процестер тізіміне қосу; • алдыңғы тексеруден кейінгі күйі өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету; • жеке тапсырма арқылы өз модульдерінің тұтастығының ықтимал бұзылуын тексеру; • сервердің маңызды аймақтарын жеке тапсырма ретінде тексеруді теңшеу; • тапсырмалардың басымдығына байланысты сервер ресурстарын антивирус пен басқа қолданбалар арасында бөлуді реттеу; • антивирустық сканерлеуді фондық режимде жалғастыру; • маңызды оқиғалар туралы әкімшілерге хабарлаудың бірнеше тәсілінің болуы (электрондық пошта хабарламасы, дыбыстық ескерту, қалқымалы терезе, оқиғалар журналына жазу); • рұқсаттар тізімдері арқылы қолданба параметрлері мен қызметіне рөлдік қол жеткізу, зиянды бағдарламалар, қаскүнемдер немесе біліктілігі жоқ пайдаланушылар тарапынан қорғауды өшіруге жол бермеу, сондай-ақ антивирусты басқаруға тыйым салу немесе рұқсат беру; • SIEM жүйелерімен интеграция; • антивирустың жұмыс процестерінің санын қолмен көрсету; • графикалық интерфейсті өшіру; • қашықтағы және жергілікті басқару консолінің болуы; • антивирус параметрлерін командалық жолдан басқару; • жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару; • операциялық жүйенің желілік экранын басқару, ережелердің бастапқы күйін қалпына келтіру мүмкіндігі; • кіріс трафигін желілік шабуыл белгілерінің
--	--

	болуына талдауды қамтамасыз ететін желілік қауіптерден қорғау; • бағдарлама процестерін сыртқы қауіптерден қорғауды қосу немесе өшіру (әдепкі бойынша функция қосулы). Функция қосулы болған кезде бағдарлама өзінің процестерін, сондай-ақ Әкімшілендіру агентінің процестерін бөгде процестердің араласуынан қорғайды; • құрылғыларды, оның ішінде желілік карталар мен модемдерді бақылау; • веб-бақылау; • пошта қауіптерінен қорғау (Outlook үшін плагин); • HTTP және HTTPS трафигін вирустар мен фишингтен қорғау, зиянды веб-мекенжайлар базалары бойынша сілтемелерді тексеру және веб-серверлер сертификаттарының жарамдылығын тексеру мүмкіндігі, трафикті ұстап қалу драйвер арқылы немесе оны қайта бағыттау арқылы жүзеге асырылуы тиіс; • барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді жасау; • арнайы ережелерді жасау бағдарламаларды олардың орналасу жолы, метадеректері, сертификаты немесе оның отпечатогы, бақылау сомасы бойынша бақылауы тиіс; • арнайы ережелер қара немесе ақ тізім режимінде, сондай-ақ статистика жинау немесе бұғаттау режимінде жұмыс істеуі тиіс, олардың ішіндегі файлдарды өзгерте және іске қоса алатын сенімді жаңарту пакеттерінің тізімін жасау мүмкіндігі болуы тиіс; • сыртқы енгізу/шығару құрылғыларымен жұмыс істеуді бақылау, сенімді құрылғылар тізімін жасау мүмкіндігі және Active Directory жүйесінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалануға артықшылықтар беру мүмкіндігі; • Интернет желісімен жұмысты бақылау, оның ішінде белгілі бір мазмұндағы ресурстарға, өндіруші алдын ала жасаған және динамикалық түрде жаңартылатын санаттарға қол жеткізуге нақты тыйым салуды немесе рұқсат беруді қосу; • сыртқы құрылғылардың қосылғаны туралы әкімшіге хабарлау; • құрылғылар мен қолданбаларды бақылау ережелерін автоматты түрде жасау механизмдерінің болуы. Мобильді құрылғыларға арналған антивирустық қорғаудың бағдарламалық құралдарына
--	--

	қойылатын талаптар Смартфондарды антивирустық қорғауға арналған бағдарламалық құралдар мынадай мобильді ОЖ басқаруында жұмыс істеуі тиіс: - о Android 5.0 және одан жоғары (Android 12L қоса алғанда, Go Edition қоспағанда); - о iOS 10 және одан жоғары немесе iPadOS 13 және одан жоғары; Android ОЖ арналған смартфондарды антивирустық қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • антивирустық қорғау құралдарын өндірушінің бұлттық репутациялық сервисін пайдалана отырып, қосымша тексеру деңгейі бар смартфонның файлдық жүйесін тұрақты антивирустық қорғау; • құрылғының файлдық жүйесін сұрау бойынша және кесте бойынша тексеру; • орнатылатын қолданбаларды лезде тексеру; • антивирустық қорғау құралдарын өндірушінің бұлттық репутациялық сервисінің вердикттері негізінде зиянды және фишингтік сайттарды бұғаттау; • вирус жұққан объектілерді оқшаулауға арналған қойманың болуы; • зиянды бағдарламаларды іздеу және қауіпті объектілерді жою кезінде пайдаланылатын антивирустық базаларды кесте бойынша жаңарту; • көрсетілген қолданбаларды, оның ішінде алдын ала белгіленген қолданбалар санаттары арқылы іске қосуды бұғаттау; • рұқсат етілген қолданбалардың ақ тізімдерін қолдау; • қолданбаларды іске қосуды бақылау шеңберінде жүйелік қолданбаларды бұғаттау; • Firebase Cloud Messaging (FCM) сервисі арқылы командалар мен push-хабарламаларды жіберу; • wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануды бұғаттау; • wi-fi желілеріне қосылу параметрлерін көрсету; • орнатуға міндетті қолданбаларды көрсету; • мобильді құрылғыны бұғаттау, деректерді жою, жұмыс қызметіне байланысты деректерді жою, құрылғының орналасқан жерінің координаталарын алу, зауыттық параметрлерге қашықтан қайтару (factory reset); • корпоративтік саясаттарға сәйкестігін тексеру жүргізілетін ережелер тізімін жасау, сәйкессіздіктер анықталған жағдайда құрылғыны автоматты түрде бұғаттау, деректерді жою, корпоративтік қолданбаларды іске қосуға тыйым
--	--

	салу мүмкіндігі; • Samsung KNOX1 және KNOX2 технологияларын қолдау; • Android-құрылғыларға арналған Қолданбаларды бақылау ережелерін жасау кезінде қолданбалардың рұқсат етілген нұсқаларын көрсету. Apple iOS ОЖ арналған смартфондарды қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • топтық саясаттардың көмегімен iOS MDM-құрылғыларының параметрлерін қашықтан теңшеу; • деректерді бұғаттау және жою командасын жіберу; • мобильді құрылғылардың қауіпсіздік топтық саясаттарын жасау; • Exchange ActiveSync\ iOS MDM хаттамасы арқылы қосылған құрылғылардың конфигурациялық параметрлерін қашықтан теңшеу; • пайдаланушылардың мобильді құрылғыларының жұмысы туралы есептер мен статистиканы алу; • supervised mode режимін пайдаланған кезде антивирустық қорғау құралдарын өндірушінің бұлттық репутациялық сервистерінің вердикттері негізінде зиянды және фишингтік сайттарды бұғаттау; • бірыңғай басқару консолі арқылы орталықтандырылған басқару; • басқарылатын құрылғыда iTunes, Safari немесе Game Center сияқты құрылғының жеке қолданбаларын пайдалануға болатынын бақылауға мүмкіндік беретін компоненттің болуы; • iOS MDM-құрылғылары үшін Bluetooth параметрлерін өзгертуге тыйым салу. Windows жұмыс станциялары мен серверлеріне арналған шабуылдарды тергеу және әрекет ету бағдарламалық құралдарына қойылатын талаптар Жұмыс станциялары мен серверлерге арналған шабуылдарды тергеу және әрекет ету бағдарламалық құралдары әзірлеушінің антивирустық шешімінің құрамында кіріктірілген мамандандырылған агент түрінде жеткізілуі және мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс: • агенттің бағдарламалық құрал әзірлеушісінің антивирустық шешімдерімен үйлесімділігі; • мынадай ОЖ-ларға орнатуды қолдау: - o Windows 7 Home / Professional / Ultimate /
--	--

	Enterprise Service Pack 1 және одан жоғары; - o Windows 8 Professional / Enterprise (32 / 64-разрядты); - o Windows 8.1 Professional / Enterprise (32 / 64-разрядты); - o Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise/Enterprise multi-session; - o Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise - o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 және одан жоғары; - o Windows Server 2012 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; - o Windows Server 2016 Essentials / Standard / Datacenter; - o Windows Server 2019 Essentials / Standard / Datacenter; - o Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Core Mode қоса алғанда) • бағдарламалық құрал әзірлеушісінің антивирустық шешімінен жаңа анықтаулар бойынша кеңейтілген ақпаратты мынадай түрде ұсыну: - o қауіптің даму тізбегінің графы; - o қауіп анықталған құрылғы туралы IP-мекенжайды, MAC, ОЖ нұсқасын, құрылғы атауын, пайдаланушылар тізімін қамтитын ақпарат; - o анықтау туралы жалпы ақпарат, оның ішінде анықталған уақыт, объект атауы, бар болған жағдайда объектіні іске қосу параметрлері, объектінің орналасқан каталогы, оның MD5 және SHA256 бақылау сомалары, есептік жазба атауы, анықтау режимі (мысалы, сұрау бойынша сканерлеу кезінде немесе автоматты сканерлеу кезінде анықтау); - o анықталған объект туралы кеңейтілген ақпаратты көру үшін әзірлеушінің веб-ресурсына (Threat Intelligence) сілтеме; - o анықтауға байланысты тізілімдегі өзгерістер, жасалған файлдар, іске қосылған процестер, желілік қосылымдар туралы ақпарат; - o бағдарламалық құрал әзірлеушісінің антивирустық шешімі қабылдаған жауап әрекеттері туралы ақпарат. • анықталған қауіптерге инцидент карточкасынан жауап беруді қамтамасыз ету, ізделетін құрылғы үшін немесе бірден құрылғылар тобы үшін мынадай тапсырмаларды автоматтандырылған орындау және саясаттарды қолдану негізінде:
--	--

	o alert орын алған құрылғыны оқшаулау; o файлды карантинге орналастыру; o IOC іздеу тапсырмасын жасау; o анықталған файлды іске қосуға тыйым салу; o құрылғыдағы процесті аяқтау; o құрылғыдағы процесті іске қосу; o файлды алу; o файлды жою. • компрометация индикаторлары (IOC) анықталған кезде ізделетін құрылғы үшін немесе бірден құрылғылар тобы үшін анықталған қауіптерге жауап беру мүмкіндігін қамтамасыз ету; o құрылғыны желілік оқшаулау; o маңызды аймақтарды тексеруді іске қосу; o көшірмені карантинге орналастыру, объектіні жою; • кейіннен құрылғыларда сканерлеу үшін бағдарламалық құрал әзірлеушісінің антивирустық шешімі жасаған анықтаудан компрометация индикаторларын (IOC) мынадай объектілер негізінде қалыптастыру мүмкіндігін қолдау: o файл сипаттамасы (бақылау сомасы/файл орналасқан жері); o тізілім жолдары мен кілттері; • OpenIOC форматында компрометация индикаторларын (IOC) экспорттау және импорттауды қолдау; • анықтау туралы егжей-тегжейлер сенім тобы, цифрлық қолтаңба, файлдың таралуы туралы деректерді қамтуы тиіс; • зиянды белсенділікті анықтау үшін файлдарды бұлттық оқшауланған ортада іске қосу және осы технология үшін жеке есептегішті қосу мүмкіндігі; • қауіптерге жауап беру функцияларына арналған кеңестердің болуы; • компрометация индикаторлары анықталған кезде ұйым инфрақұрылымының қауіпсіздігін қамтамасыз ету бойынша қадамдық нұсқаулықтың болуы; • кесте бойынша немесе сұрау бойынша берілген компрометация индикаторлары (IOC) бойынша құрылғыда немесе құрылғылар тобында көрсетілген аймақтарды сканерлеуді жүзеге асыру үшін арнайы тапсырма жасау, сканерлеу нәтижелерін көру мүмкіндігі; • шешіммен жұмыстың сипатталған барлық сценарийлерін орталықтандырылған басқару құралының веб-интерфейсі арқылы қолдау. Мас жұмыс станцияларына арналған шабуылдарды тергеу және әрекет ету бағдарламалық құралдарына қойылатын
--	--

	талаптар Жұмыс станциялары мен серверлерге арналған шабуылдарды тергеу және әрекет ету бағдарламалық құралдары әзірлеушінің антивирустық шешімінің құрамында кіріктірілген мамандандырылған агент түрінде жеткізілуі және мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс: • агенттің бағдарламалық құрал әзірлеушісінің антивирустық шешімдерімен үйлесімділігі; • мынадай ОЖ-ларға орнатуды қолдау: - o macOS 12-15; • бағдарламалық құрал әзірлеушісінің антивирустық шешімінен жаңа анықтаулар бойынша кеңейтілген ақпаратты мынадай түрде ұсыну: - o қауіп анықталған құрылғы туралы IP-мекенжайды, MAC және ОЖ нұсқасын қамтитын ақпарат; - o анықтау туралы жалпы ақпарат, оның ішінде анықталған уақыт, объект атауы, бар болған жағдайда объектіні іске қосу параметрлері, объектінің орналасқан каталогы, оның MD5 және SHA256 бақылау сомалары, есептік жазба атауы, анықтау режимі (мысалы, сұрау бойынша сканерлеу кезінде немесе автоматты сканерлеу кезінде анықтау); - o анықталған объект туралы кеңейтілген ақпаратты көру үшін әзірлеушінің веб-ресурсына (Threat Intelligence) сілтеме; - o анықтауға байланысты тізілімдегі өзгерістер, жасалған файлдар, іске қосылған процестер, желілік қосылымдар туралы ақпарат; - o бағдарламалық құрал әзірлеушісінің антивирустық шешімі қабылдаған жауап әрекеттері туралы ақпарат. • анықталған қауіптерге инцидент карточкасынан жауап беруді қамтамасыз ету, ізделетін құрылғы үшін немесе бірден құрылғылар тобы үшін мынадай тапсырмаларды автоматтандырылған орындау және саясаттарды қолдану негізінде: - o alert орын алған құрылғыны оқшаулау; - o файлды карантинге орналастыру; - o IOC іздеу тапсырмасын жасау; - o анықталған файлды іске қосуға тыйым салу; - o құрылғыдағы процесті аяқтау; - o құрылғыдағы процесті іске қосу; - o файлды алу; - o файлды жою. • компрометация индикаторлары (IOC) анықталған кезде ізделетін құрылғы үшін немесе
--	---

	бірден құрылғылар тобы үшін анықталған қауіптерге жауап беру мүмкіндігін қамтамасыз ету: - о құрылғыны желілік оқшаулау; - о маңызды аймақтарды тексеруді іске қосу; - о көшірмені карантинге орналастыру, объектіні жою; • кейіннен құрылғыларда сканерлеу үшін бағдарламалық құрал әзірлеушісінің антивирустық шешімі жасаған анықтаудан компрометация индикаторларын (ИОС) мынадай объектілер негізінде қалыптастыру мүмкіндігін қолдау: - о файл сипаттамасы (бақылау сомасы/файл орналасқан жері); - о тізілім жолдары мен кілттері; • OpenИОС форматында компрометация индикаторларын (ИОС) экспорттау және импорттауды қолдау; • анықтау туралы егжей-тегжейлер сенім тобы, цифрлық қолтаңба, файлдың таралуы туралы деректерді қамтуы тиіс; • зиянды белсенділікті анықтау үшін файлдарды бұлттық оқшауланған ортада іске қосу және осы технология үшін жеке есептегішті қосу мүмкіндігі; • қауіптерге жауап беру функцияларына арналған кеңестердің болуы; • компрометация индикаторлары анықталған кезде ұйым инфрақұрылымының қауіпсіздігін қамтамасыз ету бойынша қадамдық нұсқаулықтың болуы; • кесте бойынша немесе сұрау бойынша берілген компрометация индикаторлары (ИОС) бойынша құрылғыда немесе құрылғылар тобында көрсетілген аймақтарды сканерлеуді жүзеге асыру үшін арнайы тапсырма жасау, сканерлеу нәтижелерін көру мүмкіндігі; • шешіммен жұмыстың сипатталған барлық сценарийлерін орталықтандырылған басқару құралының веб-интерфейсі арқылы қолдау. Linux жұмыс станциялары мен серверлеріне арналған шабуылдарды тергеу және әрекет ету бағдарламалық құралдарына қойылатын талаптар Жұмыс станциялары мен серверлерге арналған шабуылдарды тергеу және әрекет ету бағдарламалық құралдары әзірлеушісінің антивирустық шешімінің құрамында кіріктірілген мамандандырылған агент түрінде жеткізілуі және мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс: • агенттің бағдарламалық құрал әзірлеушісінің
--	---

	антивирустық шешімдерімен үйлесімділігі; 32-биттік операциялық жүйелердің мынадай нұсқаларына орнатуды қолдау: o Debian GNU/Linux 11.0 және одан жоғары. o Debian GNU/Linux 12.0 және одан жоғары. o Mageia 4. o Альт 8 СП Рабочая Станция (8.4). o Альт 8 СП Сервер (8.4). 64-биттік операциялық жүйелердің мынадай нұсқаларына орнатуды қолдау: o AlmaLinux OS 8 және одан жоғары. o AlmaLinux OS 9 және одан жоғары. o AlterOS 7.5 және одан жоғары. o Amazon Linux 2. o Astra Linux Common Edition 2.12. o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5). o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6). o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7). o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6). o Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6). o Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7). o CentOS 7.2 және одан жоғары. o CentOS Stream 8. o CentOS Stream 9. o Debian GNU/Linux 11.0 және одан жоғары. o Debian GNU/Linux 12.0 және одан жоғары. o EMIAS 1.0 және одан жоғары. o EulerOS 2.0 SP10. o Kylin 10. o Linux Mint 21.1 және одан жоғары. o Linux Mint 22.0 және одан жоғары. o Mostech 12. o openSUSE Leap 15.0 және одан жоғары. o Oracle Linux 7.3 және одан жоғары. o Oracle Linux 8.0 және одан жоғары. o Oracle Linux 9.0 және одан жоғары. o Red Hat Enterprise Linux 7.2 және одан жоғары. o Red Hat Enterprise Linux 8.0 және одан жоғары. o Red Hat Enterprise Linux 9.0 және одан жоғары. o Rocky Linux 8.5 және одан жоғары. o Rocky Linux 9.0 және одан жоғары. o SberLinux 9.0.1. o SberOS 3.3.3. o SUSE Linux Enterprise Server 12.5 және одан жоғары. o SUSE Linux Enterprise Server 15 және одан жоғары.
--	---

	- o Ubuntu 22.04 LTS. - o Ubuntu 24.04 LTS. - o Альт 8 СП Рабочая станция (8.4). - o Альт 8 СП Сервер (8.4). - o Альт Образование 10.1. - o Альт СП Рабочая Станция релиз 10. - o Альт СП Рабочая Станция релиз 10.1. - o Альт СП Сервер релиз 10. - o Альт СП Сервер релиз 10.1. - o Атлант, сборка Alcyone, версия 2022.02. - o Гослинукс 7.17. - o Гослинукс 7.2. - o М ОС 12 Сервер. - o МОС ОС 15.4 Арбат. - o МСВСФЕРА АРМ 9.2 және одан жоғары. - o МСВСФЕРА СЕРВЕР 9.2 және одан жоғары. - o ОС МЭШ 12 Для всех пользователей (без телеметрии и без поддержки ДИТ). - o ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ). - o ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ). - o ОСнова 2.9 және одан жоғары. - o РЕД ОС 7.3. - o РЕД ОС 8.0. - o РОСА "Кобальт" 7.9. - o РОСА "Хром" 12. - o СинтезМ-Клиент 8.6. - o СинтезМ-Сервер 8.6. ARM архитектурасына арналған 64-bitтік операциялық жүйелерге орнатуды қолдау: - o Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7). - o CentOS Stream 9. - o EulerOS 2.0 SP10. - o SUSE Linux Enterprise Server 15. - o Ubuntu 22.04 LTS. - o Альт СП Рабочая Станция релиз 10. - o Альт СП Сервер релиз 10. - o РЕД ОС 7.3. - o РЕД ОС 8.0. • бағдарламалық құрал әзірлеушісінің антивирустық шешімінен жаңа анықтаулар бойынша кеңейтілген ақпаратты мынадай түрде ұсыну: - o қауіптің даму тізбегінің графы; - o қауіп анықталған құрылғы туралы IP-мекенжайды, MAC және ОЖ нұсқасын қамтитын ақпарат; - o анықтау туралы жалпы ақпарат, оның ішінде анықталған уақыт, объект атауы, бар болған жағдайда объектіні іске қосу параметрлері,
--	---

	объектінің орналасқан каталогы, оның MD5 және SHA256 бақылау сомалары, есептік жазба атауы, анықтау режимі (мысалы, сұрау бойынша сканерлеу кезінде немесе автоматты сканерлеу кезінде анықтау); - o анықталған объект туралы кеңейтілген ақпаратты көру үшін әзірлеушінің веб-ресурсына (Threat Intelligence) сілтеме; - o анықтауға байланысты тізілімдегі өзгерістер, жасалған файлдар, іске қосылған процестер, желілік қосылымдар туралы ақпарат; - o бағдарламалық құрал әзірлеушісінің антивирустық шешімі қабылдаған жауап әрекеттері туралы ақпарат. • анықталған қауіптерге инцидент карточкасынан жауап беруді қамтамасыз ету, ізделетін құрылғы үшін немесе бірден құрылғылар тобы үшін мынадай тапсырмаларды автоматтандырылған орындау және саясаттарды қолдану негізінде: - o alert орын алған құрылғыны оқшаулау; - o файлды карантинге орналастыру; - o IOC іздеу тапсырмасын жасау; - o анықталған файлды іске қосуға тыйым салу; - o құрылғыдағы процесті аяқтау; - o құрылғыдағы процесті іске қосу; - o файлды алу; - o файлды жою. • компрометация индикаторлары (IOC) анықталған кезде ізделетін құрылғы үшін немесе бірден құрылғылар тобы үшін анықталған қауіптерге жауап беру мүмкіндігін қамтамасыз ету: - o құрылғыны желілік оқшаулау; - o маңызды аймақтарды тексеруді іске қосу; - o көшірмені карантинге орналастыру, объектіні жою; • кейіннен құрылғыларда сканерлеу үшін бағдарламалық құрал әзірлеушісінің антивирустық шешімі жасаған анықтаудан компрометация индикаторларын (IOC) мынадай объектілер негізінде қалыптастыру мүмкіндігін қолдау: - o файл сипаттамасы (бақылау сомасы/файл орналасқан жері); - o тізілім жолдары мен кілттері; • OpenIOC форматында компрометация индикаторларын (IOC) экспорттау және импорттауды қолдау; • анықтау туралы егжей-тегжейлер сенім тобы, цифрлық қолтаңба, файлдың таралуы туралы деректерді қамтуы тиіс; • зиянды белсенділікті анықтау үшін файлдарды бұлттық оқшауланған ортада іске қосу және осы
--	--

	технология үшін жеке есептегішті қосу мүмкіндігі; • қауіптерге жауап беру функцияларына арналған кеңестердің болуы; • компрометация индикаторлары анықталған кезде ұйым инфрақұрылымының қауіпсіздігін қамтамасыз ету бойынша қадамдық нұсқаулықтың болуы; • кесте бойынша немесе сұрау бойынша берілген компрометация индикаторлары (IOC) бойынша құрылғыда немесе құрылғылар тобында көрсетілген аймақтарды сканерлеуді жүзеге асыру үшін арнайы тапсырма жасау, сканерлеу нәтижелерін көру мүмкіндігі; • шешіммен жұмыстың сипатталған барлық сценарийлерін орталықтандырылған басқару құралының веб-интерфейсі арқылы қолдау. Windows ОЖ базасындағы орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қойылатын талаптар Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары мынадай нұсқалардағы операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі тиіс: - o Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядты. - o Windows Server 2016 Standard/Datacenter/Essentials/Server Core (орнату нұсқалары) (LTSB) 64-разрядты. - o Windows Server 2019 Standard/Datacenter/Core 64-разрядты. - o Windows Server 2022 Standard/Datacenter/Core 64-разрядты. - o Windows Storage Server 2019 64-разрядты. Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары мынадай виртуалды платформаларға орнатуды қолдауы тиіс: - o VMware vSphere 6.7. - o VMware vSphere 7.0. - o Microsoft Hyper-V Server 2019 64-разрядты. - o Microsoft Hyper-V Server 2022 64-разрядты. - o Citrix XenServer 7.1 LTSR. - o Citrix XenServer 8.x. - o Parallels Desktop 18. - o Oracle VM VirtualBox 7.x. Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары мынадай нұсқалардағы ДҚБЖ-мен жұмыс істеуі тиіс: - o Microsoft SQL Server 2016 (барлық редакциялары)
--	---

	64-разрядты. - o Microsoft SQL Server 2017 (барлық редакциялары) Windows/Linux үшін 64-разрядты. - o Microsoft SQL Server 2019 (барлық редакциялары) Windows/Linux үшін 64-разрядты (қосымша әрекеттер талап етіледі). - o Microsoft SQL Server 2022 (барлық редакциялары) Windows/Linux үшін 64-разрядты. - o MySQL 5.7 Community 32-разрядты/64-разрядты. - o MySQL Standard Edition 8.0 (8.0.20 және одан жоғары релизи) 32-разрядты/64-разрядты. - o MySQL Enterprise Edition 8.0 (8.0.20 және одан жоғары релизи) 32-разрядты/64-разрядты. - o MariaDB 10.5 (10.5.27 және одан жоғары құрастырылымы) 32-разрядты/64-разрядты. - o MariaDB Galera Cluster 10.3 32-разрядты/64-разрядты, InnoDB сақтау ішкі жүйесімен. - o PostgreSQL 13.x 64-разрядты. - o PostgreSQL 14.x 64-разрядты. - o PostgreSQL 15.x 64-разрядты. - o Postgres Pro 13.x Windows/Linux 64-разрядты. - o Postgres Pro 14.x Windows/Linux 64-разрядты. Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • қорғалатын тораптар санына байланысты орталықтандырылған басқару, мониторинг және жаңарту құралын орнату архитектурасын таңдау; • ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында Active Directory-ден ақпаратты оқу; • анықталған компьютерлерді IP-мекенжайы, ОЖ типі, AD OU-да орналасуы бойынша ауыстыру ережелерін теңшеу; • желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтары бойынша автоматты бөлу; IP-мекенжайы, ОЖ типі, AD OU-да орналасуы бойынша ауыстыру ережелерін теңшеу мүмкіндігі; • антивирустық қорғаудың бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою; • орталықтандырылған теңшеу, әкімшілендіру; • қорғау құралдарының жұмысы туралы есептер мен статистикалық ақпаратты қарау; • үйлесімсіз қолданбаларды басқару орталығының құралдарымен орталықтандырылған жою (қолмен және автоматты); • саясаттар мен тапсырмалар өзгерістерінің
--	---

	тарихын сақтау, алдыңғы нұсқаларға кері қайтару мүмкіндігі; • антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін – RPC, GPO, басқару жүйесінің құралдарымен, жергілікті орнату үшін – автономды орнату пакетін жасау мүмкіндігі; • қауіпсіздік саясаттарында пайдаланушы жүйеге кірген есептік жазбаға, ағымдағы IPv4-мекенжайына, сондай-ақ компьютер орналасқан OU-ға немесе қауіпсіздік тобына байланысты антивирустық шешім параметрлерін қайта анықтайтын арнайы триггерлерді көрсету; • қайта бөлу жүзеге асырылатын триггерлер иерархиясы; • жүктелген жаңартуларды клиенттік машиналарға таратпас бұрын орталықтандырылған басқару бағдарламалық құралымен тестілеу; • жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу; • желіде виртуалды машиналарды тану және осы машиналар бір физикалық серверде орналасқан жағдайда іске қосылатын тапсырмалар жүктемесінің теңгерімін олардың арасында бөлу; • әкімшілер мен операторлардың құқықтарын, сондай-ақ әр деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігі бар көпдеңгейлі басқару жүйесін құру; • еркін деңгейдегі әкімшілендіру серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі; • басқару серверлері үшін мультиарендалықты (multi-tenancy) қолдау; • бағдарламалық құралдар мен антивирустық базаларды әртүрлі көздерден, байланыс арналары арқылы да, ақпараттың машиналық тасымалдағыштарынан да жаңарту; • басқару сервері арқылы антивирустық бағдарламалық қамтамасыз ету өндірушісінің бұлттық серверлеріне қол жеткізу; • лицензияны клиенттік компьютерлерге автоматты түрде тарату; • пайдаланушылар компьютерлерінде орнатылған бағдарламалық қамтамасыз ету мен жабдықты инвентаризациялау; • орнатылған антивирустық қорғау қолданбаларының жұмысындағы оқиғалар туралы хабарлау механизмі және олар туралы электрондық пошта хабарламаларын жіберуді теңшеу; • iOS MDM сервері арқылы мобильді құрылғыларды
--	---

	басқару функциясы; • белгіленген оқиғалар туралы SMS-хабарламалар жіберу; • басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; • басқару жүйесіне түсетін желілік жүктемені азайту үшін ұйымның кез келген компьютерін жаңартуларды ретрансляциялау орталығы ретінде белгілеу; • басқару жүйесіне түсетін желілік жүктемені азайту үшін клиенттік компьютерлердің таңдалған тобының антивирустық агенттерінен оқиғаларды орталықтандырылған басқару серверіне жіберу орталығы ретінде ұйымның кез келген компьютерін белгілеу; • антивирустық қорғау оқиғалары, инвентаризация деректері, орнатылған бағдарламаларды лицензиялау деректері бойынша графикалық есептер құру; • жүйе жұмысы туралы алдын ала теңшелген стандартты есептердің болуы; • есептерді PDF және XML форматтарындағы файлдарға экспорттау; • антивирустық бағдарламалық қамтамасыз ету орнатылған барлық желі ресурстарындағы резервтік қоймалар мен карантиндер объектілерін орталықтандырылған басқару; • басқару серверінде аутентификациялау үшін ішкі есептік жазбалар жасау; • басқару жүйесінің кіріктірілген құралдарымен басқару жүйесінің резервтік көшірмесін жасау; • Windows Failover Clustering қолдауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы; • өзіне-өзі қызмет көрсету порталы пайдаланушылардың басқару агентін мобильді құрылғыға орнату мақсатында қосылу, мобильді құрылғыларды қарау, бұғаттау командаларын жіберу, құрылғыны іздеу және пайдаланушының мобильді құрылғысындағы деректерді жою мүмкіндігін қамтамасыз етуі тиіс; • вирустық эпидемиялардың туындауын бақылау жүйесінің болуы; • Microsoft Azure және Google Cloud бұлттық инфрақұрылымдарында орнату; • OpenAPI бойынша интеграция; • антивирустық қорғауды WEB-консоль арқылы басқару; • басқару консолі арқылы Windows ОЖ орналастыруды басқару мүмкіндігі; • орталықтандырылған басқару құралдары
--	--

	пайдаланушыларының алдын ала теңшелген рөлдерінің болуы; • пайдаланушылардың есептік жазбаларына байланыстыру үшін нақты көрсетілген өкілеттіктер жиынтығы бар мамандандырылған рөлдерді жасау мүмкіндігі іске асырылуы тиіс; • басқару консолінен RDP немесе штаттық құралдар арқылы қосылу мүмкіндігі; • Windows жұмыс үстеліне бірлесіп қосылу мүмкіндігінің болуы (Windows Desktop Sharing); • пайдаланушыға қашықтан қосылуға рұқсат беру туралы сұрау көрсетілуі тиіс; • ОЖ образдарымен жұмыс істеу құралдарының болуы: физикалық немесе виртуалды машина негізінде мақсатты ОЖ образын жасау, образды әкімші таңдаған компьютерлерге, оның ішінде "таза аппараттық құралға" (bare metal) орнату; • бұрын жасалған образға драйверлер жиынтығын қосу мүмкіндігі қамтамасыз етілуі тиіс; • ОЖ орнатылғаннан кейін автоматты режимде скрипттерді іске қосу немесе қосымша бағдарламалық қамтамасыз етуді орнату мүмкіндігі; • операциялық жүйе образын дистрибутивтерден (WIM) импорттау мүмкіндігі; • компьютерде орнатылған үшінші тарап бағдарламалық қамтамасыз ету лицензияларын бақылау жүйесінің болуы, лицензияны пайдалану бұзылғаны немесе лицензияның қолданылу мерзімі асып кеткені туралы әкімшіге хабарлау мүмкіндігі; • үшінші тарап қолданбалары үшін орнату пакеттерін (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) автоматты түрде жасау және осы қолданбалар пакеттерін компьютерлерге автоматты орталықтандырылған орнату; • деректерді шифрлауды басқару функционалын қолдау; • SIEM жүйелерімен интеграциялау және оқиғаларды syslog немесе CEF\ LEEF форматында беру мүмкіндігі; • Әкімшілендіру консоліне рұқсатсыз қол жеткізу тәуекелін азайту үшін екі кезеңді тексеру; • пайдаланушының есептік жазбасы параметрлері өзгертілгеннен кейін қосымша аутентификацияны пайдалану; • IPv6 және IPv4-мекенжайларымен жұмыс істеу және IPv6-мекенжайлары бар құрылғылар орналасқан желілерді сұрау мүмкіндігі; • пайдаланушылар компьютерлерінде орнатылған қолданбалар мен операциялық жүйедегі осалдықтарды автоматтандырылған
--	--

	іздеу және жою; • Әкімшілендіру серверін жоғары қолжетімділік жүйесі ретінде орналастыру мүмкіндігі; • оқшауланған желіде үшінші тарап өндірушілерінің бағдарламаларына жаңартуларды орнату және осалдықтарды жабу мүмкіндігі (Microsoft бағдарламаларын қоспағанда); • Windows және Linux базасындағы клиенттік құрылғыларды қашықтан диагностикалау (трассировкаларды, оқиғалар журналдарын, дамπτарды алу, қолданбаларды тоқтату және іске қосу); • Linux операциялық жүйесі бар басқарылатын құрылғылардағы жергілікті әкімші есептік жазбаларының құқықтарын қайтарып алу мүмкіндігі; • Linux операциялық жүйесі бар басқарылатын құрылғылардағы жергілікті есептік жазбаның паролін өзгерту мүмкіндігі. Linux ОЖ базасындағы орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қойылатын талаптар Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары мынадай нұсқалардағы операциялық жүйелерді басқаратын компьютерлерде жұмыс істеуі тиіс: - o Debian GNU/Linux 11.x (Bullseye) 64-разрядты. - o Debian GNU/Linux 12 (Bookworm) 64-разрядты. - o Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядты. - o Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядты. - o CentOS Stream 9 64-разрядты. - o Red Hat Enterprise Linux Server 7.x 64-разрядты. - o Red Hat Enterprise Linux Server 8.x 64-разрядты. - o Red Hat Enterprise Linux Server 9.x 64-разрядты. - o SUSE Linux Enterprise Server 12 (барлық жаңарту пакеттері) 64-разрядты. - o SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) 64-разрядты. - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядты. - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядты. - o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядты. - o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядты. - o Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядты. - o Astra Linux Special Edition РУСБ.10015-03
--	---

	(обновление 7.6) 64-разрядты. - o Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядты. - o Astra Linux Common Edition (очередное обновление 2.12) 64-разрядты. - o Альт СП Сервер 10 64-разрядты. - o Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядты. - o Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядты. - o Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядты. - o Альт СП Рабочая станция 10 64-разрядты. - o Oracle Linux 7 64-разрядты. - o Oracle Linux 8 64-разрядты. - o Oracle Linux 9 64-разрядты. - o Platform V SberLinux OS Server (SLO) 8.9.2 64-разрядты. - o РЕД ОС 7.3 Сервер 64-разрядты. - o РЕД ОС 7.3 Сертифицированная редакция 64-разрядты. - o РЕД ОС 8 64-разрядты. - o РОСА "КОБАЛЬТ" 7.9 64-разрядты. - o М ОС (Moscow Electronic School) 12 Сервер 64-разрядты. - o Mostech Server 64-разрядты. - o МосОС 15.4 Arbat 64-разрядты. Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары мынадай виртуалды платформаларға орнатуды қолдауы тиіс: - o VMware vSphere 6.7.0. - o VMware vSphere 7.0.3. - o Microsoft Hyper-V Server 2019 64-разрядты. - o Microsoft Hyper-V Server 2022 64-разрядты. - o Citrix XenServer 7.x. - o Citrix XenServer 8.2. - o Parallels Desktop 18. - o Oracle VM VirtualBox 7.0.12. - o Kernel-based Virtual Machine (барлық қолдау көрсетілемін Linux ОЖ). Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары мынадай нұсқалардағы ДҚБЖ-мен жұмыс істеуі тиіс: - o MySQL 5.7 Community 32-разрядты/64-разрядты. - o MySQL Standard Edition 8.0 (8.0.20 және одан жоғары релизі) 32-разрядты/64-разрядты. - o MySQL Enterprise Edition 8.0 (8.0.20 және одан жоғары релизі) 32-разрядты/64-разрядты. - o MariaDB 10.1 (10.1.30 және одан жоғары құрастырылымы) 32-разрядты/64-разрядты. - o MariaDB 10.3 (10.3.22 және одан жоғары құрастырылымы) 32-разрядты/64-разрядты. - o MariaDB 10.4 (10.4.20 және одан жоғары құрастырылымы) 32-разрядты/64-разрядты.
--	--

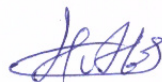
	о MariaDB 10.5 (10.5.27 және одан жоғары құрастырылымы) 32-разрядты/64-разрядты. о MariaDB 10.6 (10.6.20 және одан жоғары құрастырылымы) 32-разрядты/64-разрядты. о MariaDB 10.11 (10.11.10 және одан жоғары құрастырылымы) 32-разрядты/64-разрядты. о MariaDB Galera Cluster 10.3 32-разрядты/64-разрядты, InnoDB сақтау ішкі жүйесімен. о PostgreSQL 13.x 64-разрядты. о PostgreSQL 14.x 64-разрядты. о PostgreSQL 15.x 64-разрядты. о PostgreSQL 15.x 64-разрядты (Corosync/Pacemaker кластері). о PostgreSQL 16.x 64-разрядты. о PostgreSQL 17 64-разрядты. о Postgres Pro 13.x (барлық редакциялары) 64-разрядты. о Postgres Pro 14.x (барлық редакциялары) 64-разрядты. о Postgres Pro 15.x (барлық редакциялары) 64-разрядты. о Postgres Pro 15.x 64-разрядты (Corosync/Pacemaker кластері). о Postgres Pro 16.x (барлық редакциялары) 64-разрядты. о Postgres Pro 16.x Enterprise 64-разрядты (Built-in High Availability кластері). о Postgres Pro 17 (барлық редакциялары) 64-разрядты. о Postgres Pro 17 Enterprise 64-разрядты (Built-in High Availability кластері). о Platform V Pangolin 5.4.0 64-разрядты. о Jatoba 4 64-разрядты. Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: • антивирустық қорғаудың бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою; • орталықтандырылған теңшеу, әкімшілендіру; • қорғау құралдарының жұмысы туралы есептер мен статистикалық ақпаратты қарау; • саясаттар мен тапсырмалар өзгерістерінің тарихын сақтау, алдыңғы нұсқаларға кері қайтару мүмкіндігі; • қайта бөлу жүзеге асырылатын триггерлер иерархиясы; • жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу; • желіде виртуалды машиналарды тану және осы машиналар бір физикалық серверде орналасқан жағдайда іске қосылатын тапсырмалар жүктемесінің теңгерімін олардың арасында бөлу;
--	---

	• әкімшілер мен операторлардың құқықтарын, сондай-ақ әр деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігі бар көпдеңгейлі басқару жүйесін құру; • еркін деңгейдегі әкімшілендіру серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі; • басқару серверлері үшін мультиарендалықты (multi-tenancy) қолдау; • бағдарламалық құралдар мен антивирустық базаларды әртүрлі көздерден, байланыс арналары арқылы да, ақпараттың машиналық тасымалдағыштарынан да жаңарту; • басқару сервері арқылы антивирустық бағдарламалық қамтамасыз ету өндірушісінің бұлттық серверлеріне қол жеткізу; • лицензияны клиенттік компьютерлерге автоматты түрде тарату; • орнатылған антивирустық қорғау қолданбаларының жұмысындағы оқиғалар туралы хабарлау механизмі және олар туралы электрондық пошта хабарламаларын жіберуді теңшеу; • антивирустық қорғау оқиғалары, орнатылған бағдарламаларды лицензиялау деректері бойынша графикалық есептер құру; • жүйе жұмысы туралы алдын ала теңшелген стандартты есептердің болуы; • есептерді PDF және XML форматтарындағы файлдарға экспорттау; • антивирустық бағдарламалық қамтамасыз ету орнатылған барлық желі ресурстарындағы резервтік қоймалар мен карантиндер объектілерін орталықтандырылған басқару; • басқару серверінде аутентификациялау үшін ішкі есептік жазбалар жасау; • басқару жүйесінің кіріктірілген құралдарымен басқару жүйесінің резервтік көшірмесін жасау; • вирустық эпидемиялардың туындауын бақылау жүйесінің болуы; • антивирустық қорғауды WEB-консоль арқылы басқару; • антивирустық базалар мен бағдарламалық модульдерді басқарылатын құрылғыларға әкімшілендіру сервері арқылы да, әкімшілендіру серверіне түсетін жүктемені азайту және корпоративтік желідегі деректер трафигін оңтайландыру үшін тарату нүктелері арқылы да жаңарту және тарату мүмкіндігі; • жаңартуларды тексеру тапсырмасы арқылы жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын олардың жұмысқа қабілеттілігін және қателердің болуын тексеру
--	--

	мүмкіндігі; • антивирустық базалар мен бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары функциясын пайдалану мүмкіндігі; • негізгі Сервер ретінде жұмыс істеу және Linux немесе Windows операциялық жүйелері бар Серверлерді бағынышты ретінде басқару; • оқиғалар іріктемелерін экспорттау және импорттау; • басқарылатын құрылғыларда орнатылған бағдарламалар туралы ақпарат алу; • Microsoft Active Directory және Samba домен контроллерлері бойынша құрылғыларды іздеу мүмкіндігі; • Windows ОЖ басқаруындағы әкімшілендіру серверінен Linux ОЖ басқаруындағы әкімшілендіру серверіне деректерді автоматтандырылған тасымалдау мүмкіндігі; • басқарылатын құрылғыларды қашықтан диагностикалау мүмкіндігі; • кластерлік технологияны қолдау; • басқарылатын құрылғылардан үйлесімсіз бағдарламалық қамтамасыз етуді орталықтандырылған жою мүмкіндігі. Антивирустық базаларды жаңартуға қойылатын талаптар Жаңартылатын антивирустық дерекқорлар мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс: • антивирустық базаларды жаңарту ережелерін күнтізбелік тәулік ішінде кемінде 24 рет жасау; • жаңарту жолдарының көптігі, оның ішінде байланыс арналары және ажыратылатын электрондық ақпарат тасымалдағыштары арқылы; • жаңартулардың тұтастығы мен түпнұсқалығын электрондық цифрлық қолтаңба құралдарымен тексеру. Пайдалану құжаттамасына қойылатын талаптар • Антивирустық құралдармен бірге жеткізілетін құжаттама тиісті антивирустық қорғау құралын орнату, теңшеу және пайдалану процесін егжей-тегжейлі сипаттауы тиіс. Техникалық қолдауға қойылатын талаптар Антивирустық бағдарламалық қамтамасыз етудің техникалық қолдауы: • Қазақстан Республикасының бүкіл аумағында антивирустық қорғау құралдарын өндірушінің және оның серіктестерінің сертификатталған мамандары орыс тілінде электрондық пошта және Интернет арқылы ұсынуы тиіс. • Антивирустық шешім өндірушісінің Web-сайты орыс тілінде болуы, антивирустық шешімді
--	--

	• жаңарту жолдарының көптігі, оның ішінде байланыс арналары және ажыратылатын электрондық ақпарат тасымалдағыштары арқылы; • жаңартулардың тұтастығы мен түпнұсқалығын электрондық цифрлық қолтаңба құралдарымен тексеру. Пайдалану құжаттамасына қойылатын талаптар • Антивирустық құралдармен бірге жеткізілетін құжаттама тиісті антивирустық қорғау құралын орнату, теңшеу және пайдалану процесін егжей-тегжейлі сипаттауы тиіс. Техникалық қолдауға қойылатын талаптар Антивирустық бағдарламалық қамтамасыз етудің техникалық қолдауы: • Қазақстан Республикасының бүкіл аумағында антивирустық қорғау құралдарын өндірушінің және оның серіктестерінің сертификатталған мамандары орыс тілінде электрондық пошта және Интернет арқылы ұсынуы тиіс. • Антивирустық шешім өндірушісінің Web-сайты орыс тілінде болуы, антивирустық шешімді техникалық қолдауға арналған арнайы бөлімі, үнемі толықтырылып отыратын білім базасы, сондай-ақ бағдарламалық өнімдерді пайдаланушылар форумы болуы тиіс. • Жеткізуші жеткізілетін бағдарламалық өнімнің кіріспе курсы бойынша нұсқама жүргізеді. Кіріспе курс практикалық сабақтармен бекітіледі, электрондық әдістемелік құралдар ұсынылады. Кіріспе курс аяқталғаннан кейін Жеткізуші тыңдаушыларға сертификат береді. Кіріспе курс шарт жасалғаннан кейін бір ай ішінде өткізіледі. • Қызмет шеңберінде Жеткізуші антивирустық бағдарламалық қамтамасыз етуді және тиісті қорғау компоненттерін орнатуды орындауы тиіс; • орнатудан кейін қорғаудың негізгі компоненттерінің дұрыс жұмыс істеуін тексеру;
--	--

Цифрлық трансформация және жүйелерді дамыту
департаментінің басшысы



А. Хамитжан