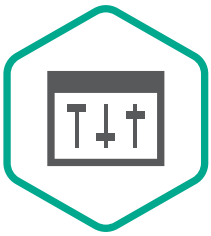
kaspersky АКТИВИРУЙ БУДУЩЕЕ



Kaspersky Security Center

Гибкие возможности управления системой безопасности

Kaspersky Security Center упрощает управление безопасностью и администрирование IT-систем, а также удовлетворяет потребности в защите, которые изменяются вместе с вашей компанией. Единая универсальная консоль позволяет управлять всеми IT-системами и безопасности, а также облегчает разделение обязанностей между администраторами.

Признанный лидер
В 2017 г. «Лаборатория Касперского» приняла участие в 86 независимых обзорах. В 72 случаях наши продукты были признаны лучшими и 78 раз они оказались в первой тройке.

Концепция Kaspersky HuMachine
Сочетание возможностей машинного обучения, глобальной аналитики больших данных и опыта экспертов, накопленного за два десятилетия, обеспечивает оптимальную защиту и эффективность работы.

Сеть Kaspersky Security Network
Облачная сеть безопасности Kaspersky Security Network – это сложная распределенная инфраструктура, которая обеспечивает максимально быстрое реагирование на новые угрозы, повышая эффективность защитных компонентов и минимизируя риск ложных срабатываний.

Единая консоль управления

Благодаря тому, что абсолютное большинство наших защитных технологий поддерживают управление из единой консоли управления – Kaspersky Security Center, ваши специалисты по IT-безопасности смогут быстрее и проще применять политики безопасности на всех рабочих местах. Централизованное управление дополняется доступом на основе ролей, поэтому каждый администратор сможет обращаться только к тем инструментам и данным, которые имеют отношение к его служебным обязанностям.

Простое масштабирование

Поддерживается масштабирование без изменения первоначальной настройки – один экземпляр сервера Kaspersky Security Center обеспечивает управление до 100 000 физических, виртуальных и облачных рабочих мест с оптимизированными возможностями резервного копирования.

Расширяемая архитектура

Расширяемая архитектура Kaspersky Security Center включает плагины для управления продуктами безопасности для каждой платформы. В случае приобретения или выпуска нового приложения можно установить соответствующее расширение в Kaspersky Security Center без повторной установки или исправления консоли.

Преимущества

Централизация управления безопасностью позволяет добиться большей прозрачности, снизить расходы и повысить эффективность администрирования. Kaspersky Security Center содержит инструменты и технологии, которые в сочетании образуют передовую интегрированную платформу для обеспечения безопасности.

Упрощает выполнение повседневных задач

Средства развертывания, конфигурирования и администрирования защиты для рабочих мест обеспечивают безопасность всех устройств в сети на основе последних данных.

Уменьшает уязвимость к атакам

Средства централизованного контроля веб-ресурсов, приложений и устройств позволяют ограничить использование неподходящих или небезопасных приложений, устройств и веб-сайтов.

Помогает защитить все рабочие места и серверы

Windows, Linux, Mac, Android, iOS, физические и виртуальные серверы и рабочие места – все это можно защищать и администрировать из одной консоли.

Обеспечивает безопасность мобильных устройств

Поддерживает централизованное администрирование средств защиты для основных платформ мобильных устройств для повышения прозрачности и улучшения контроля без привлечения дополнительных ресурсов или технологий.

Распространяет надежную защиту на облачные среды

Встроенная интеграция между консолью управления и облачной средой Amazon Web Services (AWS) обеспечивает полную прозрачность и контроль приложений безопасности на основе Linux и Windows Server, развернутых в облаке.

Облегчает администрирование

Средства расширенного клиентского управления автоматизируют и централизуют выполнение административных задач, в том числе ведение учета программного и аппаратного обеспечения, создание образов, удаленное развертывание ПО и устранение неполадок.

Предоставляет полный обзор IT-среды

Kaspersky Security Center передает и ретранслирует команды, сообщения и информацию между сервером Endpoint Detection and Response (EDR), который осуществляет поиск признаков вторжения на каждом узле в режиме реального времени, и агентом Endpoint Protection для обеспечения повышенной прозрачности и безопасности.

Упрощает установку исправлений

Компонент автоматической оценки уязвимостей и управления установкой исправлений позволяет удаленно развертывать стороннее ПО, а круглосуточный доступ к аналитическим данным обеспечивает своевременное обновление потенциально уязвимого ПО, освобождая IT-администраторам время для других задач.

Расширяет возможности поставщиков управляемых услуг

Kaspersky Security Center поддерживает корпоративное лицензирование на основе подписки и работу с несколькими клиентами. Неограниченная поддержка виртуальных серверов администрирования и возможности удаленного управления через веб-консоль обеспечивают гибкое управление IT-инфраструктурами нескольких компаний-клиентов.

Обеспечивает целостность систем

Kaspersky Security Center позволяет отслеживать любые изменения критически важных активов, таких как веб-серверы и банкоматы, а также своевременно реагировать на нарушения целостности этих систем.

Упрощает развертывание

Мастера для управления корпоративными мобильными устройствами (EMM) позволяют развертывать средства защиты с использованием технологии удаленной установки ПО (OTA), сторонних систем EMM и консолей развертывания (Samsung KNOX)

Основные возможности

Установка «из коробки» и готовая к использованию конфигурация

Централизация управления безопасностью позволяет добиться большей прозрачности, снизить расходы и повысить эффективность администрирования. Kaspersky Security Center содержит инструменты и технологии, которые в сочетании образуют передовую интегрированную платформу для обеспечения безопасности.

Не только управление защитой от угроз

Комплексное управление физическими, виртуальными и облачными рабочими местами из единой консоли повышает эффективность, снижает совокупную стоимость эксплуатации и предоставляет другие возможности.

- Поддерживается создание и администрирование политик безопасности для устройств под управлением Windows, Linux и Mac OS.
- Можно использовать Kaspersky Security Network для управления облачной защитой.
- Централизованное управление Контролем программ, Контролем устройств и Веб-Контролем обеспечивает надежную защиту.
- Доступно управление системой предотвращения вторжений (HIPS).
- Поддерживается настройка параметров сетевого экрана и управление ими в операционных системах Linux и Windows.
- Настройка шифрования с использованием Kaspersky Encryption, Microsoft BitLocker и FileVault позволяет защитить данные в случае потери или кражи устройств. Политики шифрования можно согласовывать с параметрами контроля приложений и устройств.

Удобное управление защитой мобильных устройств

Управляйте мобильными устройствами, включая Android и iOS, так же, как и другими рабочими местами. Администраторам доступны следующие возможности.

- С помощью решения можно управлять доступом сотрудников в интернет с мобильных устройств, блокировать вредоносные и нежелательные веб-сайты и защищать пользователей от фишинговых сайтов, похищающих информацию и идентификационные данные.
- Решение предотвращает доступ несанкционированно перепрошитых устройств к корпоративным приложениям и данным.
- Кроме того, в случае непредвиденных обстоятельств администратор или пользователь (через портал самообслуживания) может активировать меры защиты информации, в числе которых – определение местонахождения, блокирование и очистка устройства.
- Настроив доступ к функциям MDM на различных платформах через единый интерфейс, можно развернуть универсальные политики безопасности для мобильных устройств.

Поддержка виртуальных сред

Распознавание виртуальных машин и распределение нагрузки при выполнении интенсивных операций позволяют избежать «шквальных» антивирусных проверок, снижающих производительность среды, – при помощи одной консоли управления. Неважно, используете ли вы защиту без агента или легкий агент: консоль Kaspersky Security Center обеспечит полное управление защитными приложениями.

Поддержка облачных сред

Двусторонняя интеграция с решением «Лаборатории Касперского» для защиты от целевых атак позволяет не только использовать почтовые системы как дополнительный источник информации для обнаружения целенаправленных атак, но также блокировать дальнейшее распространение сообщений с опасным содержимым в зависимости от результатов глубокого анализа Kaspersky Anti Targeted Attack Platform.

Системные требования
Самую полную и актуальную версию требований см. в Базе знаний.

Общие требования
- ЦП с рабочей частотой 1,4 ГГц или выше
- 4 ГБ памяти (ОЗУ)
- 10 ГБ свободного пространства на диске

Операционные системы
- Microsoft Windows 10, 8.1, 8, 7
- Microsoft Windows Server 2016, 2012 R2, 2012
- Microsoft Small Business Server 2011
- Microsoft Windows Server 2008 R2, 2008 SP1, 2008

Интеграция с отдельными решениями

Использование интеграции с различными отдельными решениями позволяет контролировать защиту встроенных систем, шлюзов, почтовых систем и платформ совместной работы. С помощью единой консоли можно просматривать информацию о подключении и состоянии и получать доступ к сводной статистике для всех серверов и других компонентов защиты, используемых в организации.

Оптимизированное управление IT-ресурсами

Широкий диапазон возможностей управления IT-системами позволяет оптимизировать задачи управления IT-ресурсами в гетерогенных сетях.

- Все аппаратное и программное обеспечение в сети автоматически обнаруживается, благодаря чему администратор получает полное представление обо всех ресурсах, которые нуждаются в защите и управлении.
- Автоматическое развертывание ПО позволяет свести к минимуму усилия, требуемые для настройки новых устройств и установки новых приложений.
- Развертывание ПО можно выполнять по запросу администратора или запланировать на нерабочее время, а для настройки устанавливаемого программного пакета доступны дополнительные параметры.
- Решение поддерживает удаленный доступ к клиентам для устранения неполадок, в том числе механизмы авторизации, а также журналы сеансов удаленного доступа.
- Контроль создания, хранения и копирования защищенных образов систем позволяет оптимизировать и ускорять развертывание ОС. Поддерживается интерфейс UEFI.

Встроенные оптимальные процедуры аудита

Kaspersky Security Center регистрирует и сохраняет все изменения настроек, политик и задач, а также управляемых приложений для сравнения версий и выполнения отката (если потребуется). Возможности аудита позволяют администраторам сравнивать две политики с последующим созданием отчета, содержащего информацию о совпадающих и различающихся параметрах.

Улучшенные средства создания отчетов

Доступен просмотр широкого диапазона готовых и настраиваемых отчетов с применением динамической фильтрации и сортировки отчетов по любому полю.

Веб-консоль управления

Веб-консоль обеспечивает удаленное управление рабочими местами и мобильными устройствами.

Модель на основе ролей

Назначайте различные задачи по управлению безопасностью и системами разным администраторам через средство контроля доступа на основе ролей, настраивая консоль управления так, чтобы каждый администратор мог использовать только те инструменты и данные, которые соответствуют его обязанностям.

Управление уязвимостями и установкой исправлений

Используйте включенные в Kaspersky Security Center возможности управления уязвимостями и установкой исправлений, чтобы выявлять возможные пути проникновения вредоносных программ, определяя уязвимости в приложениях или операционных системах, а затем блокируйте их, не дожидаясь кибератаки. Также доступны следующие возможности.

- Поддерживается приоритизация уязвимостей и автоматическое распространение исправлений и обновлений для продуктов компании Microsoft и другого ПО.
- Можно удаленно устранять неполадки при обновлении для любых физических компьютеров, виртуальных машин или машин Amazon EC2.
- Удаленная рабочая станция может использоваться в качестве агента обновления, что сокращает объем трафика при передаче обновлений в удаленные офисы.
- Доступен мониторинг статуса установки исправлений с помощью отчетов об успешном применении исправлений.

www.kaspersky.ru