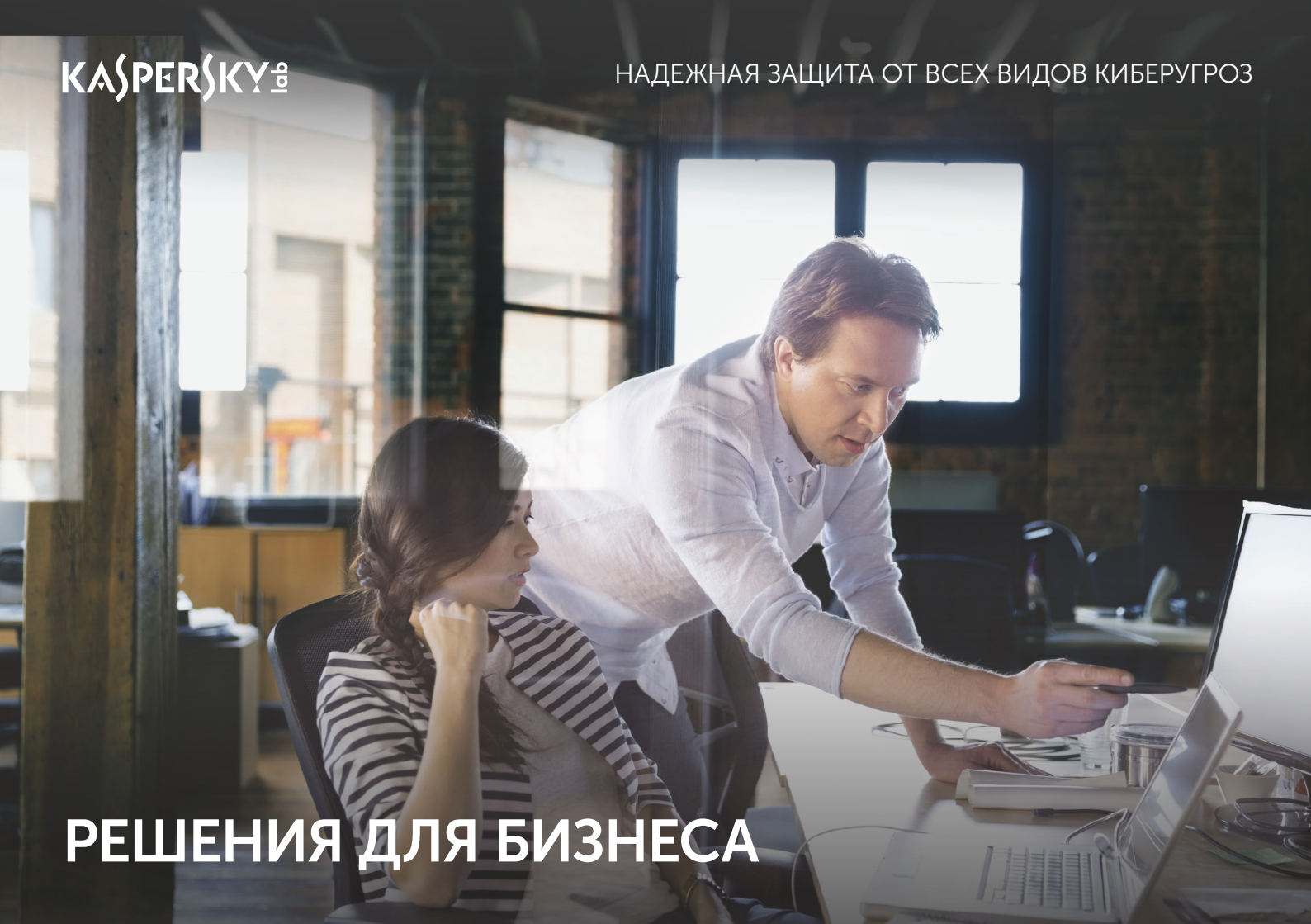
KASPERSKY lab

НАДЕЖНАЯ ЗАЩИТА ОТ ВСЕХ ВИДОВ КИБЕРУГРОЗ



РЕШЕНИЯ ДЛЯ БИЗНЕСА

Содержание

ЗАЩИТА БИЗНЕСА СЕГОДНЯ — ЭТО ВКЛАД В БЕЗОПАСНОЕ ЗАВТРА

Каждый день миллиарды людей работают с различными данными и передают их через интернет. Обмен информацией между компаниями, их сотрудниками, клиентами и поставщиками происходит непрерывно по всему миру. Это дает бизнесу очевидные преимущества, но одновременно создает дополнительные риски для информационной безопасности компаний.

По данным «Лаборатории Касперского», ежедневно появляется около 310 тыс. новых образцов вредоносного ПО. Вместе с этим растет ущерб от успешных кибератак. По результатам исследования*, для компаний малого и среднего бизнеса в 2017 году он составил около 1,6 млн рублей. В эту сумму входят оплата услуг привлеченных специалистов для устранения последствий, упущенные бизнес-возможности и убытки, вызванные простоем.

В этой ситуации компаниям приходится уделять особое внимание усилению защиты своей IT-инфраструктуры. Именно поэтому «Лаборатория Касперского» предлагает защитные решения, разработанные на единой технологической базе и ориентированные не только на борьбу с существующими угрозами, но и на предотвращение новых, еще не известных угроз. Помимо готовых продуктов, мы также предлагаем ряд сервисов, в том числе расширенную техническую поддержку и защиту от DDoS-атак Kaspersky DDoS Protection.

Принцип нашей работы прост: лучшая экспертиза в сочетании с лучшими технологиями позволяют обеспечить лучшую защиту корпоративной IT-инфраструктуры.

* Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского» и B2B International, 2017 год. Опрошено 4395 IT-специалистов из 25 стран по всему миру, включая Россию.

РЕШЕНИЯ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

Для малого бизнеса

Kaspersky Small Office Security

Многоуровневая защита и простое управление для небольшой компании до 25 сотрудников.

Для малого и среднего бизнеса

Облачное управление

Kaspersky Endpoint Security Cloud

Облачная консоль управления, доступная на любом подключенном к интернету устройстве.

Kaspersky Security для Microsoft Office 365

Защита нового поколения для почты в Office 365.

Локальный сервер управления

Kaspersky Security для бизнеса

Несколько уровней защиты бизнеса с нарастающим функционалом. Уже на уровне Стандартный решение обеспечивает безопасность рабочих мест, серверов и мобильных устройств, а также предлагает инструменты контроля программ, устройств и веб-трафика. На следующих уровнях к этому добавляется шифрование данных, средства системного администрирования и другие возможности.

Специализированные решения

«Лаборатория Касперского» предлагает ряд специализированных решений для защиты отдельных узлов сети: для виртуальных сред, почтовых серверов, систем хранения данных и т. д. Их можно приобрести в составе Kaspersky Security для бизнеса или отдельно.

KASPERSKY SMALL OFFICE SECURITY

Небольшие компании постоянно сталкиваются с теми же угрозами, что и крупные корпорации. Однако ресурсов у них значительно меньше — и финансовых, и кадровых. IT-отдел, как правило, отсутствует, и даже системный администратор далеко не всегда работает в штате. Именно поэтому небольшим компаниям требуется простое, комплексное и экономически эффективное решение, которое сможет противодействовать основным киберугрозам.

Kaspersky Small Office Security — это передовые технологии защиты в сочетании с простотой установки и настройки и удобством использования.

Резервное копирование и шифрование защищают от потери ценную деловую информацию.

Технология «Безопасные платежи» обеспечивает безопасные онлайн-транзакции и проверяет операционную систему на наличие уязвимостей, которые могут угрожать финансовой безопасности.

Облачная консоль управления позволяет управлять защитой компании в любое время из любой точки мира.

Защита от интернет-угроз противодействует фишингу, спаму и другим распространенным методам проникновения в корпоративную сеть.

Поддерживаемые платформы

Решение обеспечивает защиту самых распространенных платформ, используемых в небольших компаниях.

Компьютеры и ноутбуки Windows®

Файловые серверы Windows

Компьютеры и ноутбуки Mac®

Мобильные устройства Android™

Решения для бизнеса: kaspersky.ru/business

KASPERSKY ENDPOINT SECURITY CLOUD

Сегодня киберпреступники все чаще нацеливаются на малый средний бизнес, видя в нем легкую добычу. И действительно, такие компании не могут тратить на обеспечение IT-безопасности столько же, сколько крупные предприятия. Он нуждаются в готовом решении, которое просто установить и которым просто управлять — на месте или удаленно.

Kaspersky Endpoint Security Cloud отвечает этим потребностям бизнеса и предлагает защиту компьютеров, мобильных устройств и файловых серверов из облачной консоли управления, которая не требует покупки дополнительного оборудования и позволяет управлять системой безопасности компании с любого устройства, подключенного к интернету.

НАДЕЖНАЯ МНОГОУРОВНЕВАЯ ЗАЩИТА И МАКСИМАЛЬНО ПРОСТОЕ УПРАВЛЕНИЕ

- Облачная консоль, которая упрощает администрирование
- Защита компьютеров, ноутбуков и файловых серверов на базе Windows
- Безопасность мобильных устройств на базе iOS® и Android
- Предустановленные политики безопасности, разработанные экспертами
- Полностью готовое решение — не требуется покупать дополнительное оборудование
- Для сервисов-провайдеров: простое управление политиками безопасности разных компаний из единой консоли

KASPERSKY SECURITY ДЛЯ MICROSOFT OFFICE 365

Чтобы остановить бизнес, достаточно лишь одного вредоносного сообщения. Крайне важно обнаружить и заблокировать спам и опасные вложения до того, как они успеют причинить ущерб, без замедления работы или случайного удаления легитимного трафика.

Kaspersky Security для Microsoft Office 365 использует передовую эвристику, песочницу, машинное обучение и другие технологии нового поколения для защиты электронной почты от программ-вымогателей, вредоносных вложений, спама и других угроз. Как и Microsoft Office 365, решение размещается в облаке.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА РЕШЕНИЯ:

- Интуитивно понятное управление из единой облачной консоли Kaspersky Business Hub
- Отсутствие дополнительных затрат на новое оборудование
- Полный контроль процесса обработки подозрительных писем
- Передовая защита от спама, фишинга, вредоносных программ (в том числе программ-вымогателей) и эффективная фильтрация почтовых вложений

KASPERSKY SECURITY ДЛЯ БИЗНЕСА

Сегодня, в условиях роста количества и сложности киберугроз, любой компании необходимо обладать новейшими инструментами защиты и помнить о том, что большинство кибератак на предприятия начинается с использования уязвимостей устройств сотрудников. Именно эффективная защита каждого рабочего места – как стационарного, так и мобильного — создает надежную основу для реализации стратегии обеспечения безопасности.

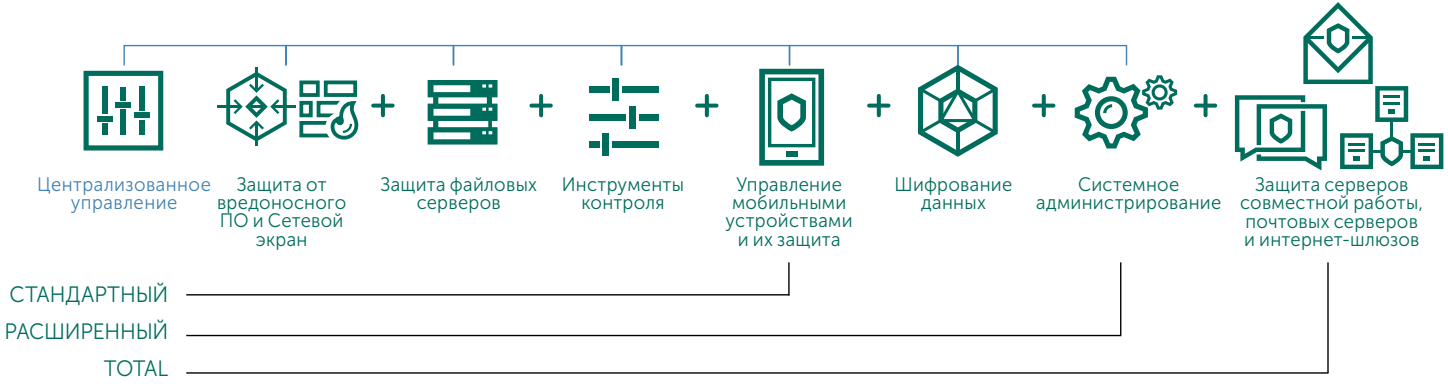
Для контроля и защиты рабочих мест, а также обеспечения безопасности периметра корпоративной сети «Лаборатория Касперского» предлагает линейку Kaspersky Security для бизнеса. Оптимальным образом подобранные инструменты и технологии формируют несколько уровней решения с нарастающим функционалом.

Kaspersky Endpoint Security для бизнеса Стандартный — защита компьютеров, ноутбуков, мобильных устройств и файловых серверов. Контроль использования программ, устройств и интернета. Защита от шифрования. Централизованное управление из единой консоли.

Kaspersky Endpoint Security для бизнеса Расширенный — инструменты уровня Стандартный, а также средства системного администрирования, шифрование данных, мониторинг уязвимостей и автоматическая установка исправлений.

Kaspersky Total Security для бизнеса — инструменты уровня Расширенный, а также защита почтовых серверов, серверов, совместной работы и интернет-шлюзов.

Уровни Kaspersky Security для бизнеса



Единая консоль

Администратор может наблюдать за состоянием защиты всех физических, виртуальных и мобильных устройств, а также управлять их безопасностью из единой консоли. Это ускоряет работу и упрощает контроль.

Единая платформа

Все ключевые технологии, функциональные компоненты и модули разрабатываются внутри компании на собственной технологической базе. Благодаря этому растет эффективность защиты, снижается нагрузка на систему и повышается стабильность работы приложений.

Единая лицензия

Вы получаете не ряд отдельных решений в рамках одной покупки, а приобретаете единое комплексное решение, в котором оптимальным образом объединены все необходимые для защиты вашего бизнеса технологии.

ЗАЩИТА ОТДЕЛЬНЫХ УЗЛОВ

Все узлы и уровни корпоративной сети нуждаются в надежной специализированной защите. «Лаборатория Касперского» предлагает ряд решений для обеспечения безопасности отдельных узлов сети. Кроме того, клиентам доступны гибкие и эффективные средства системного администрирования. Управление почти всеми защитными решениями и технологиями осуществляется с помощью единой универсальной консоли Kaspersky Security Center.

Специализированные решения для:


почтовых серверов


интернет-шлюзов


системного администрирования


файловых серверов

виртуальных и облачных сред


систем хранения данных


мобильных устройств


серверов совместной работы


защиты от DDoS-атак

Эти продукты могут приобретаться в дополнение к уровням Kaspersky Security для бизнеса или отдельно.

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ И ОБЛАЧНЫХ СРЕД

Сочетание виртуальных и облачных сред разного типа с локальными ресурсами зачастую оказывается экономически оправданным. Однако эта гибридная среда должна соответствовать жестким стандартам безопасности. В противном случае под ударом окажутся ценные данные и непрерывная работа бизнеса.

Решение Kaspersky Security для виртуальных и облачных сред позволяет организовать адаптивную экосистему кибербезопасности с продуманным управлением. Где бы вы ни хранили и обрабатывали критические бизнес-данные – в частном или общедоступном облаке либо в их сочетании, – сбалансированное сочетание гибких и эффективных средств защиты оградит ваши рабочие нагрузки от самых сложных известных и неизвестных угроз, без ущерба для производительности.

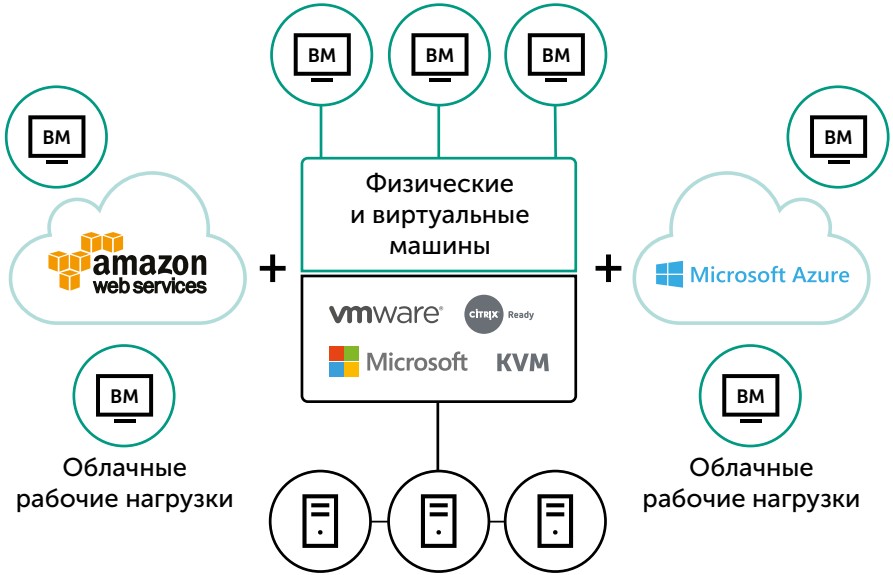
Защита нового поколения для физических, виртуальных и облачных сред

Запатентованные технологии защищают все рабочие нагрузки вне зависимости от их расположения.

- Многоуровневая постоянная защита в паре с машинным обучением отвечает за безопасность ваших данных, процессов и приложений.
- Технологии защиты виртуальных машин на основе легкого агента и без агента позволяют обезопасить программно-определяемые ЦОД без ущерба для производительности.
- Интеграция со встроенной системой безопасности общедоступных и управляемых облачных сред помогает защитить приложения, ОС, пользователей и потоки данных с минимальным расходом ресурсов.
- Объединенное управление физическими и виртуальными ресурсами повышает эффективность администрирования

ПРЕИМУЩЕСТВА KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ И ОБЛАЧНЫХ СРЕД

- Оптимизация под физические, виртуальные и облачные рабочие нагрузки
- Многоуровневая интегрированная система защиты для любого частного ЦОД
- Гармоничная интеграция гибких и автоматизированных средств безопасности с публичными облаками AWS и Azure
- Централизованное управление безопасностью всей гибридной облачной среды корпоративного класса



KASPERSKY SECURITY ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Мобильные устройства все чаще служат мишенью для атак киберпреступников. В то же время политика использования личных устройств в рабочих целях (Bring Your Own Device, BYOD) расширяет диапазон устройств в составе корпоративной сети, что усложняет администраторам контроль IT-инфраструктуры.

Kaspersky Security для мобильных устройств обеспечивает безопасность смартфона или планшета сотрудника независимо от его местонахождения. Решение защищает от постоянно развивающегося вредоносного ПО для мобильных устройств и позволяет осуществлять мониторинг и контроль смартфонов и планшетов в вашей корпоративной сети из единой консоли и с минимальным влиянием на работу пользователей.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Надежная защита от вредоносного ПО
- Защита от спама и фишинговых ссылок
- Контроль программ и Веб-Контроль
- Выявление попыток рутинга/джейлбрейкинга
- Контейнеризация
- Анти-Вор
- Управление мобильными устройствами
- Портал самообслуживания
- Централизованное управление
- Веб-консоль
- Поддержка популярных платформ: Android™, iOS® и Windows Phone®

Примечание: набор доступных функций зависит от защищаемой платформы.

ПЕРЕДОВАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Kaspersky Security для мобильных устройств сочетает защиту от вредоносного ПО с другими технологиями безопасности, что позволяет обеспечить многоуровневую защиту данных, хранящихся на мобильных устройствах, от известных и новых угроз.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ (MDM)

Интеграция со всеми основными платформами для управления мобильными устройствами позволяет осуществлять развертывание и контроль удаленно (Over-the-Air, OTA).

УПРАВЛЕНИЕ МОБИЛЬНЫМИ ПРИЛОЖЕНИЯМИ (MAM)

Технологии контейнеризации отделяют корпоративные данные от персональных, а Контроль приложений помогает определить приложения, которые разрешается использовать в корпоративной сети.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Возможность управлять мобильными устройствами на базе различных платформ через ту же единую консоль, которая служит для управления защитой остальных рабочих мест.

KASPERSKY SYSTEMS MANAGEMENT

Централизованное и автоматизированное выполнение основных задач, связанных с обеспечением безопасности, настройкой и системным администрированием рабочих мест, позволяет не только экономить время IT-специалистов, но и оптимизировать работу системы защиты. К таким задачам относятся мониторинг уязвимостей, установка исправлений и обновлений ПО, учет аппаратного и программного обеспечения, развертывание ОС и приложений и многое другое.

Kaspersky Systems Management помогает устранить риски информационной безопасности и упростить управление сложной корпоративной IT-инфраструктурой, обеспечивая IT-администраторам полный контроль безопасности многочисленных устройств, приложений и пользователей — в режиме реального времени из единой консоли управления.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Мониторинг уязвимостей и управление установкой исправлений
- Учет аппаратного и программного обеспечения
- Удаленная установка ПО и устранение неполадок, в том числе в удаленных офисах
- Развертывание операционных систем
- Интеграция с SIEM-системами
- Распределение прав администраторов на основе ролей
- Централизованное управление

ПОВЫШЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ

Оперативная автоматизированная установка исправлений и обновлений позволяет добиться повышения уровня безопасности и экономии ресурсов, требуемых для выполнения рутинных задач администрирования.

ПРОВЕРКА СЕТИ ДЛЯ УЧЕТА ПРОГРАММНОГО И АППАРАТНОГО ОБЕСПЕЧЕНИЯ

Автоматическое обнаружение, а также отслеживание аппаратного и программного обеспечения позволяют администраторам получить полную картину корпоративной сети со всеми устройствами. Автоматизированная проверка приложений позволяет быстро обнаруживать их устаревшие версии, нарушающие безопасность и требующие обновления.

ВЫЯВЛЕНИЕ И ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ

Автоматизированный поиск уязвимостей позволяет их быстро выявлять, приоритизировать и устранять. Поиск уязвимостей может выполняться не только автоматически, но и по расписанию, заданному администратором. Гибкое управление политиками облегчает распространение обновленного, совместимого ПО, а также создание исключений.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Kaspersky Systems Management является компонентом единой консоли управления Kaspersky Security Center. Доступ к каждой функции решения и работа с ней осуществляются из единой консоли. Интуитивно понятный интерфейс и единые политики позволяют полностью автоматизировать выполнение рутинных задач IT-администрирования.

ОТСЛЕЖИВАНИЕ РЕЗУЛЬТАТОВ И СОСТАВЛЕНИЕ ОТЧЕТОВ

Kaspersky Systems Management сообщает IT-администраторам о состоянии установки исправлений и позволяет им составлять отчеты по проверкам, находить потенциальные слабые места, отслеживать изменения и получать дополнительную подробную информацию о защищенности корпоративной IT-сети – а также о каждом устройстве и системе в ней.

KASPERSKY SECURITY ДЛЯ ПОЧТОВЫХ СЕРВЕРОВ

Электронная почта сегодня — это не только основное средство коммуникации в большинстве компаний, но и один из основных путей распространения спама и вредоносных программ. В результате атак, проводимых через электронную почту, многие компании лишаются ценных данных и терпят значительные убытки, а постоянный поток спама вынуждает сотрудников тратить рабочее время на удаление из своих почтовых ящиков сотен ненужных писем.

Kaspersky Security для почтовых серверов обеспечивает непревзойденную защиту почтового трафика на серверах Microsoft Exchange, Linux® и Lotus® Domino® от спама, фишинговых ссылок и вредоносного ПО, в том числе в сложных гетерогенных IT-инфраструктурах.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Защита от вредоносного ПО в режиме реального времени
- Интеграция с облаком
- Защита от уязвимостей нулевого дня
- Блокирование вредоносных ссылок и вложений
- Резервное копирование данных
- Гибкая настройка правил
- Масштабируемость
- Отказоустойчивость

Примечание: набор доступных функций зависит от защищаемой платформы.

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Передовое антивирусное ядро «Лаборатории Касперского» при поддержке облачной сети Kaspersky Security Network обеспечивает надежную защиту от вредоносных программ, проактивную защиту от эксплойтов и эффективную фильтрацию вредоносных ссылок.

ГИБКОЕ АДМИНИСТРИРОВАНИЕ

Простые и удобные в использовании инструменты управления и создания отчетов, а также гибкие настройки проверки позволяют эффективно контролировать безопасность электронной почты и документов, экономят ваши ресурсы и снижают нагрузку на IT-администраторов. Управлять приложением Kaspersky Security для Microsoft Exchange Servers можно с помощью консоли Kaspersky Security Center.

ЗАЩИТА ОТ СПАМА

Передовые антиспам-технологии «Лаборатории Касперского» позволяют обнаруживать и устранять практически весь спам, поступающий на серверы почтовой инфраструктуры компании.

ЗАЩИТА ОТ ФИШИНГА С ПОМОЩЬЮ НЕЙРОСЕТЕЙ

Предлагаемая «Лабораторией Касперского» передовая защита от фишинга опирается на нейросетевой анализ для повышения эффективности обнаружения. Эта облачная технология использует более 1000 критериев, включая анализ изображений, языковые проверки и сигнатуры скриптов, и опирается на собираемые со всего мира данные о вредоносных и фишинговых URL-адресах, чтобы защищать пользователя как от известных, так и от неизвестных фишинговых электронных писем и угроз «нулевого дня».

KASPERSKY SECURITY ДЛЯ ИНТЕРНЕТ-ШЛЮЗОВ

Безопасный интернет-доступ для всех сотрудников организации — важнейший элемент любой корпоративной стратегии безопасности.

Kaspersky Security для интернет-шлюзов – это решение мирового класса для защиты от вредоносного ПО, обеспечивающее безопасное использование интернета.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Защита от вредоносного ПО
- Гибкие настройки сканирования
- Баланс загрузки сервера
- Масштабируемость
- Отказоустойчивость
- Интуитивно понятные инструменты управления
- Подробные отчеты

ВСЕСТОРОННЯЯ ЗАЩИТА, СОКРАЩЕНИЕ ПРОСТОЕВ И ПЕРЕБОЕВ В РАБОТЕ

Решение обеспечивает всестороннюю защиту HTTP-, HTTPS- и FTP-трафика, проходящего через популярные шлюзы на базе Linux, автоматически удаляя из него вредоносные и потенциально опасные программы. Благодаря регулярным обновлениям, оптимизированному интеллектуальному сканированию в сочетании с распределением нагрузки, Kaspersky Security для интернет-шлюзов обладает высоким уровнем обнаружения угроз и практически не замедляет работу системы. Все это позволяет свести к минимуму перебои в рабочих процессах предприятия, вызванные вредоносным ПО, а также связанные с ними затраты.

ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ ЗА СЧЕТ ОПТИМИЗАЦИИ

Оптимизированная интеллектуальная технология сканирования и баланс загрузки сервера позволяют сократить потребление ресурсов и экономно использовать каналы передачи данных, одновременно поддерживая высокий уровень безопасности.

УДОБНОЕ УПРАВЛЕНИЕ И ГИБКАЯ СИСТЕМА ОТЧЕТОВ

Простые, интуитивно понятные инструменты управления, гибкие настройки проверки и подробные отчеты о статусе защиты позволяют эффективно управлять системой безопасности корпоративной IT-инфраструктуры.

KASPERSKY SECURITY ДЛЯ СЕРВЕРОВ СОВМЕСТНОЙ РАБОТЫ

Платформы, используемые для обмена файлами и данными, могут способствовать быстрому распространению вредоносного ПО и других информационных угроз в корпоративной сети.

Чтобы обеспечить безопасную и бесперебойную совместную работу с документами, «Лаборатория Касперского» разработала решение, в котором эффективные технологии защиты от вредоносных атак сочетаются с простотой управления и удобством использования.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Удостоенное наград антивирусное ядро
- Контроль доступа к данным
- Защита от фишинга
- Файловая и контентная фильтрация
- Резервное копирование данных
- Облачная защита в режиме реального времени (Kaspersky Security Network)
- Централизованное гибкое управление
- Удобная консоль администрирования

KASPERSKY SECURITY ДЛЯ ФАЙЛОВЫХ СЕРВЕРОВ

Всего один зараженный файл на корпоративном сервере может распространиться на все компьютеры локальной сети. Поэтому решение для защиты файловых серверов должно не только обеспечивать защиту важной информации, но и не позволять вредоносному ПО проникать в резервные копии файлов, что приводит к повторным заражениям.

Kaspersky Security для файловых серверов — это экономически эффективное,надежное и масштабируемое решение для защиты файловых хранилищ Windows и Linux с общим доступом, не оказывающее заметного влияния на производительность системы.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Защита от вредоносного ПО в режиме реального времени
- Интеллектуальные технологии сканирования
- Гибкие настройки проверки
- Доверенные зоны
- Централизованное управление через Kaspersky Security Center
- Карантин и резервное хранилище
- Подробные отчеты

Примечание: набор доступных функций зависит от защищаемой платформы.

ПРОАКТИВНАЯ ЗАЩИТА

Решение содержит эвристический сканер, способный обнаруживать с высокой точностью даже то вредоносное ПО, сигнатуры которого еще не были добавлены в базу данных.

ОБЛАЧНАЯ ЗАЩИТА

Облачная репутационная база данных об угрозах Kaspersky Security Network (KSN) обеспечивает скорейшее реагирование на новые угрозы, увеличивает эффективность защиты и уменьшает риск ложных срабатываний.

КОНТРОЛЬ ЗАПУСКА ПРИЛОЖЕНИЙ НА СЕРВЕРАХ

Контроль запуска приложений обеспечивает исключительную защиту. С помощью правил можно разрешить или запретить запуск исполняемых файлов, скриптов или пакетов MSI, а также загрузку на сервер модулей DLL.

ЗАЩИТА ОБЩИХ ПАПОК ОТ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ

Если на какой-либо машине замечены попытки шифрования, приложение блокирует ее доступ к любым сетевым файловым ресурсам.

ПОДДЕРЖКА РАЗЛИЧНЫХ ПЛАТФОРМ

Единое эффективное защитное решение поддерживает новейшие платформы и серверы, включая терминальные, кластерные и виртуальные, и не вызывает проблем совместимости в гетерогенных сетях.

KASPERSKY SECURITY ДЛЯ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

В условиях постоянно растущего числа угроз один-единственный зараженный файл, попавший в хранилище, подвергает риску каждый узел корпоративной сети.

Решение Kaspersky Security для систем хранения данных предлагает надежную, высокоэффективную и масштабируемую защиту ценной и конфиденциальной корпоративной информации, хранящейся в системах EMC™ (Isilon™, Celerra™ и VNX™), NetApp®, Dell™, Hitachi® NAS, IBM® System Storage® N и Oracle® ZFS Storage Appliance.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Защита систем хранения от вредоносного ПО в режиме реального времени
- Задачи проверки критических областей
- Усиление защиты с помощью облачной репутационной базы угроз Kaspersky Security Network (KSN)
- Поддержка антивирусного агента Celerra (CAVA), а также протоколов RPC и ICAP
- Гибкая настройка параметров проверки
- Масштабируемость и отказоустойчивость
- Оптимизация использования системных ресурсов
- Защита терминальных серверов
- Поддержка кластеров
- Технологии оптимизации антивирусной проверки
- Управление с помощью Kaspersky Security Center
- Отчеты о работе решения
- Поддержка протоколов SNMP/MOM

ГИБКИЕ НАСТРОЙКИ ПАРАМЕТРОВ ПРОВЕРКИ

Гибкие настройки параметров проверки поможет вам защитить корпоративную сеть и оптимизировать нагрузку на серверы. Вам доступно множество настроек, в том числе глубина защиты от вредоносного ПО и типы файлов, которые необходимо проверять или, напротив, проверять не нужно.

ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ

Высокоэффективная проверка с использованием оптимизированной технологии проверки и возможностью гибкой настройки исключений из проверки обеспечивает максимальный уровень безопасности при минимальном влиянии на работу системы.

БЕСПЕРЕБОЙНАЯ РАБОТА

Исключительная отказоустойчивость достигается благодаря тесной интеграции и слаженной работе всех компонентов решения.

ПРОСТОЕ УПРАВЛЕНИЕ

Установка и настройка защиты серверов производятся удаленно, без необходимости перезагружать систему. Управление приложением Kaspersky Security для систем хранения данных, а также другими решениями «Лаборатории Касперского» осуществляется с помощью единой консоли Kaspersky Security Center с простым, интуитивно понятным интерфейсом.

KASPERSKY DDOS PROTECTION

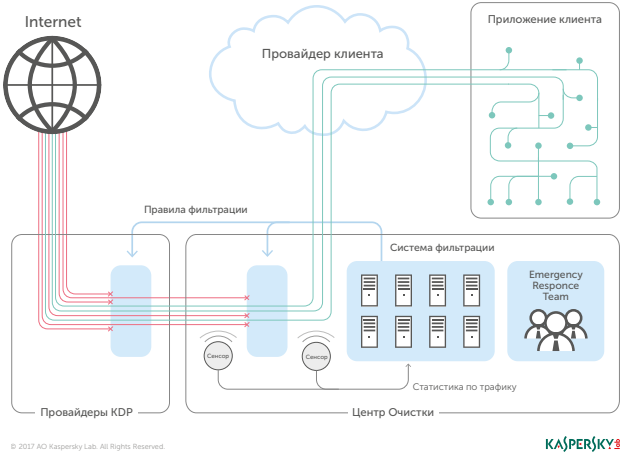
Одна DDoS-атака может обернуться многочасовыми сбоями и многомиллионными убытками. При этом стоимость проведения таких атак сегодня может составлять всего несколько тысяч рублей, а жертвой атаки может оказаться даже небольшая компания.

Решение Kaspersky DDoS Protection (KDP) способно распознавать атаки предельно быстро и борется с ними на двух фронтах: через систему мониторинга DDoS Intelligence и с помощью специальной защитной инфраструктуры «Лаборатории Касперского».

ВАРИАНТЫ ЗАЩИТЫ:

- KDP Connect – перенаправление трафика изменением DNS-записи в режиме Always On, доставка очищенного трафика через прокси-сервер, GRE-туннели или через выделенную линию.
- KDP Connect + – перенаправление трафика средствами протокола BGP в режиме Always On, доставка очищенного трафика через GRE-туннели или выделенную линию.
- KDP Control – перенаправление трафика средствами протокола BGP в режиме On Demand, доставка очищенного трафика через GRE-туннели или выделенную линию.

Схема работы Kaspersky DDoS Protection



РАСШИРЕННАЯ ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Стабильность и эффективность бизнеса во многом зависит от четкой бесперебойной работы IT-систем, поэтому мы предлагаем своим клиентам экспертную поддержку специалистов по IT-безопасности.

Соглашение о сервисном обслуживании (Maintenance Service Agreement, MSA) охватывает программы расширенной поддержки, в рамках которых решение ваших проблем в области IT-безопасности будет для специалистов «Лаборатории Касперского» приоритетной задачей.

ПОДДЕРЖКА БАЗОВОГО УРОВНЯ

Программа технической поддержки базового уровня — наглядный пример качественной поддержки по доступной цене.

Уровень MSA Start дает право на получение приоритетной поддержки по рабочим дням при возникновении критических инцидентов. Программа включает 6 премиальных инцидентов в год, с гарантированным сроком ответа 8 рабочих часов.

Для более быстрой реакции на IT-инциденты выберите уровень поддержки MSA Plus. В рамках данной программы вам гарантирован доступ к приоритетной экспертной линии поддержки для решения критических инцидентов. В пакет включено 12 премиальных инцидентов в год, с гарантированным сроком ответа 6 рабочих часов.

ПРОФЕССИОНАЛЬНЫЕ УСЛУГИ

Применяя передовой опыт и собственные эффективные методики, наши эксперты окажут поддержку во всех аспектах развертывания, настройки и обновления продуктов «Лаборатории Касперского» в вашей IT-инфраструктуре:

- **Проектирование и установка** решений «Лаборатории Касперского» для бизнеса.
- **Обучение IT-специалистов** для более эффективного использования защитных технологий «Лаборатории Касперского» с учетом особенностей IT-инфраструктуры компании.
- **Проверка состояния системы защиты** с целью оптимизации работы решения для обеспечения IT-безопасности в условиях существующей инфраструктуры с предоставлением подробного отчета и рекомендаций.

РЕШЕНИЯ ДЛЯ КРУПНОГО БИЗНЕСА

Помимо решений для малого и среднего бизнеса, «Лаборатория Касперского» предлагает профессиональные услуги и специализированные комплексные решения для защиты предприятий. Они помогают противодействовать наиболее сложным и опасным угрозам для крупных компаний.

Защита от целевых атак и сложных угроз

Kaspersky Threat Management and Defense – единая платформа по обеспечению быстрого обнаружения угроз, расследования инцидентов, реагирования и восстановления работоспособности инфраструктуры с помощью комплекса взаимосвязанных защитных решений и сервисов.

В состав решения входят: платформа по противодействию целенаправленным атакам Kaspersky Anti Targeted Attack Platform, система обнаружения инцидентов на рабочих местах и активного реагирования на них Kaspersky Endpoint Detection and Response, а также сервисы кибербезопасности.

Защита критической инфраструктуры

Kaspersky Industrial CyberSecurity – это решение, состоящее из технологий и сервисов, призванное защитить промышленные системы на каждом уровне, не нарушая непрерывности работы и не снижая стабильности технологического процесса.

Защита центров обработки данных

Решение «Лаборатории Касперского» для защиты центров обработки данных обеспечивает защиту самых распространенных гипервизоров, помогая достичь высокой степени консолидации виртуальных машин. В дополнение к этому решение эффективно защищает корпоративные сетевые хранилища данных и файловые серверы.

Защита встраиваемых систем

Kaspersky Embedded Systems Security — это специализированное решение для обеспечения безопасности кассовых систем, киосков самообслуживания и банкоматов. Оно помогает организациям соблюсти требования PCI DSS и обладает такими ключевыми для защиты встроенных систем функциями, как контроль устройств и режим «Запрет по умолчанию».

Защита мобильного и онлайн-банкинга

Решение Kaspersky Fraud Protection усиливает существующую систему безопасности банка, выводя ее на принципиально новый уровень. Оно активно блокирует попытки киберпреступников похитить данные пользователей, устраняя угрозу мошенничества до того, как она получит реальное воплощение.

Сервисы кибербезопасности

Сервисы информирования об угрозах, анализ защищенности инфраструктуры, расследование инцидентов и другие сервисы помогают быть в курсе ситуации в области кибербезопасности и своевременно защищаться от наиболее актуальных угроз.

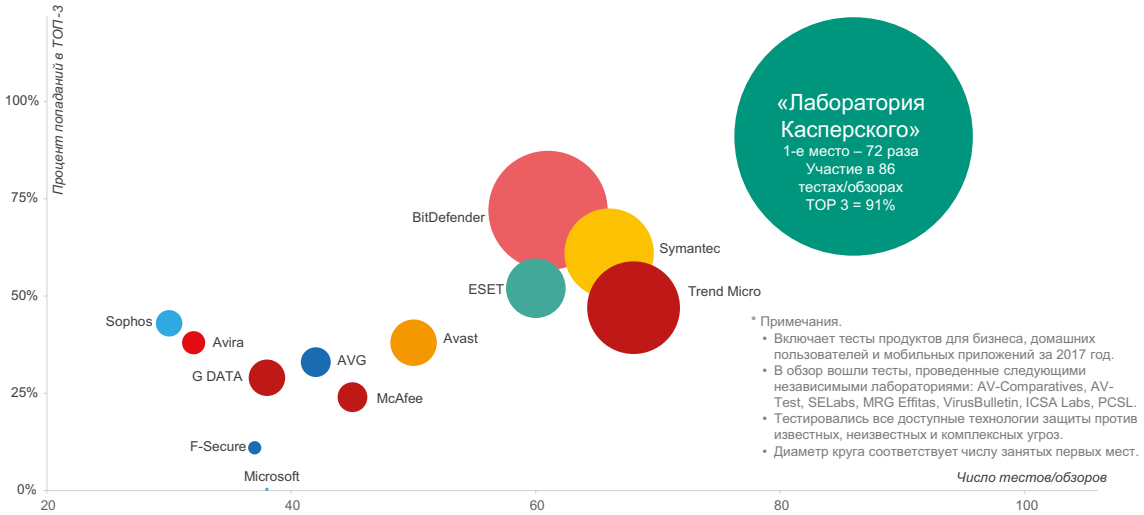
Программа повышения осведомленности

Интерактивные тренинги и платформа обучения навыкам безопасного поведения значительно повышают культуру кибербезопасности в компании, что позволяет в несколько раз сократить число инцидентов.

Подробнее о решениях для крупного бизнеса: kaspersky.ru/enterprise

РЕЗУЛЬТАТЫ НЕЗАВИСИМЫХ ТЕСТОВ

В 2017 году продукты «Лаборатории Касперского» приняли участие в 86 независимых тестах и обзорах. В 72 случаях они заняли первое место и 78 раз вошли в тройку лучших (ТОП-3).



Подробнее: kaspersky.ru/top3

О «ЛАБОРАТОРИИ КАСПЕРСКОГО»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и опыт компании лежат в основе защитных решений и сервисов, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и пользователей во всем мире.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для широкого круга пользователей. «Лаборатория Касперского» защищает домашних пользователей, небольшие компании, предприятия среднего бизнеса и крупные корпорации от всевозможных киберугроз, предлагая всем при этом удобные инструменты для управления системой безопасности.

«Лаборатория Касперского» понимает потребности небольших компаний и предлагает им многоуровневые решения, эффективные и простые в управлении. Компания также отвечает всем запросам крупных предприятий, предоставляя им комплексную платформу, которая защищает от всех типов киберугроз, обнаруживает самые сложные атаки, реагирует на любые инциденты и предвидит развитие угроз. Кроме того, компания предлагает набор специализированных решений, которые защищают все узлы корпоративной сети, включая мобильные устройства, а также способны обеспечить безопасность центров обработки данных и индустриальных сред.

Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов, помогая сохранить то, что для них важно.

Более подробная информация доступна на www.kaspersky.ru.

Для заметок

АО «Лаборатория Касперского»
www.kaspersky.ru

Решения для крупного бизнеса:
www.kaspersky.ru/enterprise

+7 (495) 737-34-12
sales@kaspersky.com