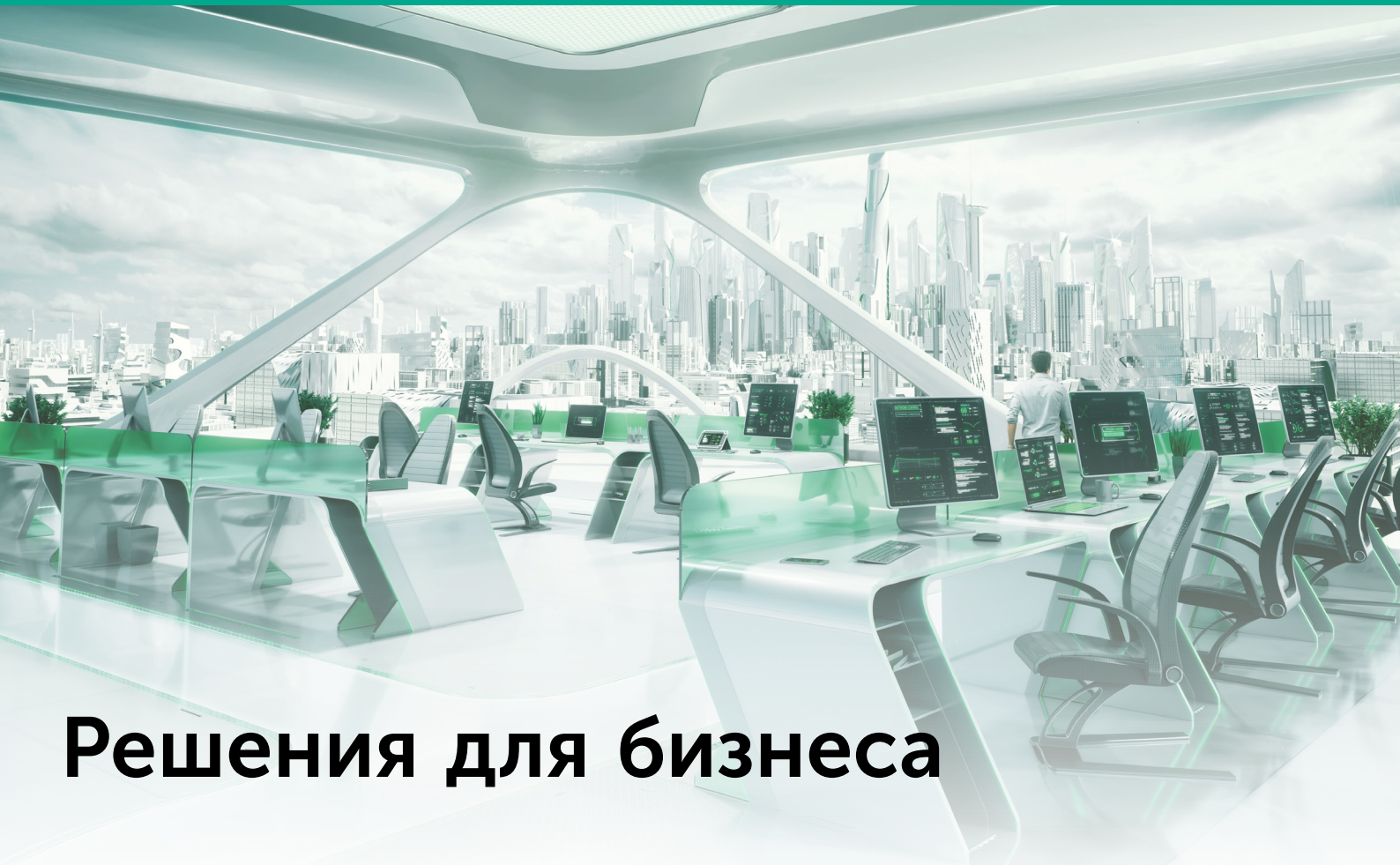
Надежная защита от всех видов киберугроз

KASPERSKY lab



Решения для бизнеса

Содержание

Защита от киберугроз для устойчивого развития бизнеса

Киберугрозы стали привычным и повседневным явлением. «Лаборатория Касперского» ежедневно фиксирует 360 тысяч новых образцов вредоносного ПО. Без надежных средств защиты от действий киберпреступников бизнес рискует — причем не только деньгами, но и стабильным развитием и репутацией. «Лаборатория Касперского» предлагает проверенные и заслужившие мировое признание продукты для защиты компаний любой величины от киберугроз любого типа и сложности.

По данным «Лаборатории Касперского», сегодня средний размер ущерба в результате всего одного инцидента для компаний среднего бизнеса составляет 4,3 млн рублей*. Размер ущерба часто настолько значителен, что компаниям приходится свертывать или корректировать долгосрочные стратегические планы. В ситуации когда бизнес становится все более и более цифровым, защита от киберугроз для компаний, нацеленных на стабильное развитие, выходит на первый план.

Решения «Лаборатории Касперского» построены на основе концепции HuMachine, которая представляет собой симбиоз машинного обучения, обработки больших данных в режиме реального времени и уникального экспертного опыта.

Благодаря этому подходу, «Лаборатория Касперского» создает передовые технологии и продукты, которые эффективны даже против сложных и ранее неизвестных киберугроз.

Портфолио продуктов «Лаборатории Касперского» для защиты бизнеса включает в себя как комплексные, так и специализированные решения для отдельных узлов сети. Они регулярно получают высокие оценки ведущих ИБ-аналитиков и побеждают в независимых тестах. А главное — они способны обеспечить защиту вашей компании и помочь ей устойчиво развиваться сегодня и в будущем.

* Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского» и B2B International, 2018 год.

Решения для защиты бизнеса

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® Endpoint Security Cloud Plus

Расширенные возможности контроля и управления из облачной консоли.

Kaspersky® Security for 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.

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™

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 управления Kaspersky Business Hub
- Защита компьютеров и ноутбуков на базе Windows и Mac
- Безопасность файловых серверов Windows
- Защита мобильных устройств на базе Android и iOS®
- 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

Сравнение основных функций двух уровней решения

	Kaspersky Endpoint Security Cloud	Kaspersky Endpoint Security Cloud Plus
Защита		
Защита от почтовых, файловых и веб-угроз	✓	✓
Сетевой экран	✓	✓
Защита от сетевых атак	✓	✓
Защита от шифровальщиков и эксплойтов	✓	✓
Анализ уязвимостей	✓	✓
Контроль и управление		
Веб-Контроль	—	✓
Контроль устройств	—	✓
Управление шифрованием	—	✓
Управление установкой исправлений	—	✓

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 Total Security для бизнеса

Наиболее комплексное решение, которое содержит защиту не только рабочих мест, но и других, потенциально уязвимых узлов – почтовых серверов и интернет-шлюзов.

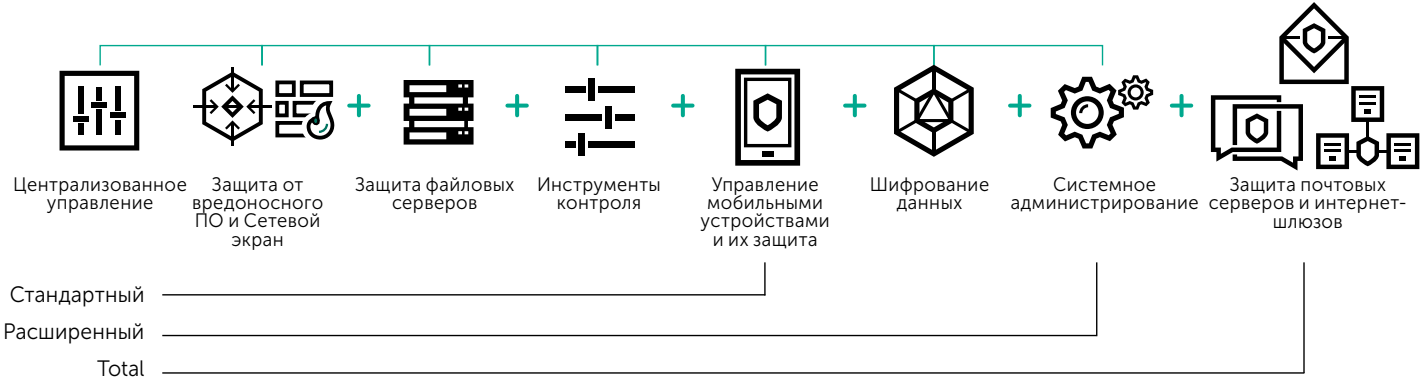
Kaspersky Endpoint Security для бизнеса Расширенный

Этот уровень решения, помимо защиты рабочих мест и серверов, содержит дополнительные возможности для защиты конфиденциальных данных и устранения уязвимостей, а также упрощает администрирование.

Kaspersky Endpoint Security для бизнеса Стандартный

Решение нового поколения, которое поможет защитить все используемые компанией рабочие места с помощью одного продукта с гибкой консолью управления.

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.

Многоуровневая защита и гибкий контроль 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.

Приложение **Kaspersky Security для мобильных устройств**, входящее в состав Kaspersky Security для бизнеса, обеспечивает безопасность смартфона или планшета сотрудника независимо от его местонахождения. Приложение 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
- Интеграция с EMM-решениями
- Анти-Вор
- Управление мобильными устройствами
- Портал самообслуживания
- Централизованное управление
- Веб-консоль
- Поддержка Android и iOS

Защита 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 приложение в составе Kaspersky Security для бизнеса 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


Точки входа
Вторжение
Заражение
Достижение целей
Предотвращение
Блокирование
Контроль выполнения
Автоматическое реагирование
Kaspersky Update Center
• Сетевая фильтрация
• Облачная контентная фильтрация
• Контроль портов
• Усиление защиты рабочих мест
• Службы репутации
• Обнаружение вредоносного ПО до выполнения
• Анализ поведения на основе машинного обучения
– Защита от эксплойтов
– Защита от программ-вымогателей
• Контроль прав на выполнение
• Автоматический откат
• Расширенное расследование
• Передовое лечение
• Активный поиск угроз
• Поиск индикаторов компрометации
• Централизованное интеллектуальное реагирование
Kaspersky Security Network
ЭТАПЫ АТАКИ
ПОРЯДОК ЗАЩИТЫ
УРОВНИ ЗАЩИТЫ

Комплексная защита вашей организации

Kaspersky Security для бизнеса использует множество технологий нового поколения – например, обработку облачных данных в режиме реального времени, анализ поведения на основе машинного обучения или защиту от эксплойтов. Они нейтрализуют большинство угроз еще до срабатывания передовых уровней защиты. Подозрительные файлы, достигающие рабочих станций, обнаруживаются и блокируются.

Защита от шифровальщиков и эксплойтов

Наши технологии постоянно развиваются благодаря машинному обучению и аналитическим данным об угрозах, поступающим в реальном времени. Защитите рабочие места от новейших эксплойтов и обезопасьте данные и общие папки от передовых угроз и вирусов-шифровальщиков.

Предотвращение кражи учетных данных

Поведенческий анализ с механизмом защиты памяти следит за критически важными системными процессами и предотвращает утечку идентификационных данных пользователей и администраторов.

Снижение уязвимости перед атаками через приложения

Контроль программ с поддержкой динамических белых списков существенно уменьшает уязвимость перед атаками «нулевого дня» благодаря полному контролю над запуском программного обеспечения на компьютерах и серверах.

Безопасный доступ к данным

Незаметное для пользователя шифрование полноценно защищает конфиденциальные данные. Интегрированная технология дает возможность централизованного применения шифрования корпоративных данных на уровне всего диска, отдельных файлов или съемного устройства и позволяет безопасно обмениваться данными в пределах сети.

Единый центр управления для всех платформ

Единая консоль обеспечивает полную видимость и контроль над всеми рабочими станциями, серверами и мобильными устройствами независимо от их расположения и состояния. Из консоли вы можете получить доступ к лицензиям, средствам удаленного устранения неполадок и настройкам сети. Функция централизованного управления дополняется интеграцией с Active Directory, ролевым доступом и встроенными панелями мониторинга.

Защита отдельных узлов сети

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

виртуальных и облачных сред


системного администрирования


систем хранения данных


защиты от DDoS-атак

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

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 трафи-ка на серверах Microsoft Exchange и Linux 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

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 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.

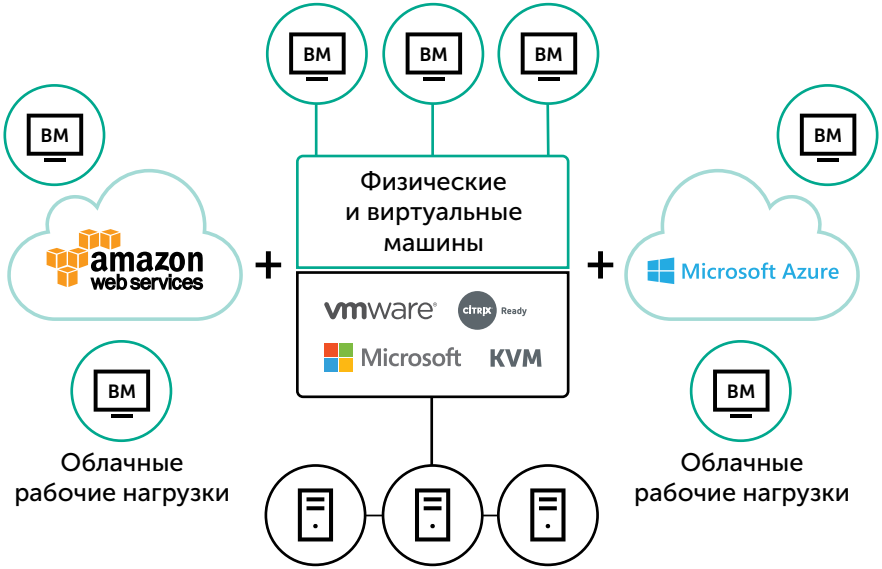
Защита нового поколения для физических, виртуальных и облачных сред

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 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 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 для бизнеса

Предотвращает нарушение бизнес-процессов

Останавливая большинство входящих угроз на уровне интернет-шлюза и не позволяя им достигать рабочих мест, Kaspersky Security для интернет-шлюзов существенно снижает нагрузку на средства защиты рабочих станций, а также уменьшает влияние человеческого фактора.

Сокращает расходы IT- и ИБ-отделов

Даже при использовании эффективной системы защиты рабочих мест, чем реже она будет сообщать об опасности, тем меньше будет волнений среди сотрудников и тем меньше времени будет уходить на расследование инцидентов.

Повышает производительность труда

Благодаря управлению использованием интернет-ресурсов решение не только уменьшает угрозу кибератак, но и ограничивает отвлекающие факторы, а также сокращает возможность использования нежелательных ресурсов. Особенно это актуально при наличии в сети устройств на платформах, отличных от Windows.

Масштабируется в соответствии с размером компании

Решение можно масштабировать в зависимости от загруженности конкретной системы, чтобы поддерживать управление несколькими узлами и иерархическое развертывание.

Снижает риски, связанные с передачей определенных типов файлов

Kaspersky Security для интернет-шлюзов повышает безопасность за счет запрета на передачу файлов определенных типов. Это позволяет предотвратить заражение вредоносным содержимым, встроенным в документы, а также снизить риск утечки данных.

Основные возможности

Сервис веб-репутации

Kaspersky Security для интернет-шлюзов включает репутационный сервис (Kaspersky Reputation Service), который обрабатывает запросы о репутации файлов, ссылок и IP-адресов, используя как данные облачной базы Kaspersky Security Network, так и локальные базы решения. Это позволяет моментально блокировать подозрительные и нежелательные файлы и веб-ресурсы.

Интеграция с SIEM-системами

Если в компании для отслеживания активности в корпоративной сети используется система управления данными и инцидентами безопасности (SIEM-система), Kaspersky Security для интернет-шлюзов расширит ее возможности с помощью экспорта информации в общий формат событий (CEF) вместе с широко используемым системным журналом.

Многоуровневая защита от различных видов киберугроз

Защита нового поколения включает несколько уровней проактивной защиты, в том числе основанных на алгоритмах машинного обучения и использовании облачных технологий. Решение обеспечивает блокирование вредоносного ПО, программ-шифровальщиков и потенциально нежелательных приложений во входящем и исходящем трафике.

Веб-контроль с использованием категорий

Для работы сотрудникам требуются далеко не все веб-ресурсы, а многие могут представлять реальную угрозу для безопасности и репутации компании (например, если на них будут размещены вредоносные или пиратские программы). Веб-контроль позволяет ограничить определенные категории веб-ресурсов для снижения рисков и обеспечения бесперебойной работы без нежелательных помех.

Контентная фильтрация

Решение позволяет запретить передачу файлов определенных типов. Для фильтрации можно использовать множество параметров, включая имя, расширение/тип (для файлов с поддельными расширениями используется распознавание формата), размер, тип MIME и хэш. Контентную фильтрацию можно использовать в различных целях, включая снижение угрозы кибератак, предотвращение утечки данных, уменьшение объема трафика и повышение производительности.

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.

Защита от спама

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 DDoS Protection

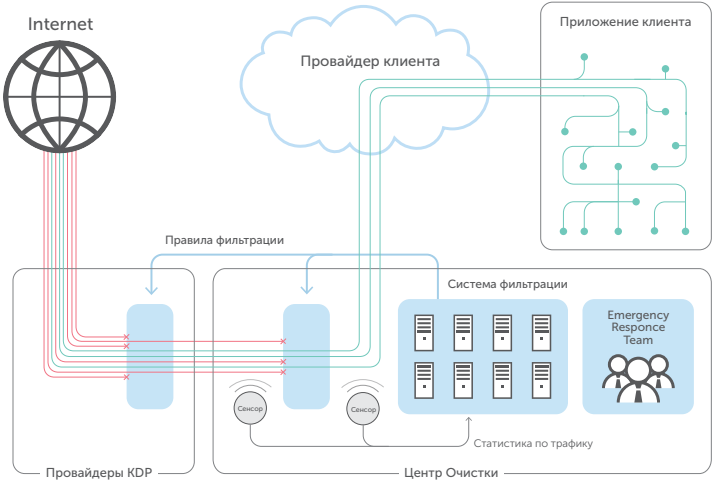
Одна DDoS-атака может обернуться многочасовыми сбоями и многомиллионными убытками. При этом стоимость проведения таких атак сегодня может составлять всего несколько тысяч рублей, а жертвой атаки может оказаться даже небольшая компания.

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 под-держки 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 & Defense

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.

Защита критической инфраструктуры

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity — набор технологий и сервисов в составе специализированного решения, призванного защитить промышленные системы на каждом уровне, не нарушая непрерывности работы и не снижая стабильности технологического процесса.

Защита встраиваемых систем

Kaspersky® Embedded Systems Security

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 от от кибермошенничества

Kaspersky® Fraud Prevention

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

Kaspersky® Cybersecurity Services

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.

Сервисы «Лаборатории Касперского»

- **Сервисы информирования об угрозах**
- **Активный поиск угроз**
- **Тренинги по кибербезопасности**
- **Сервисы реагирования на инциденты**
- **Экспертные сервисы**

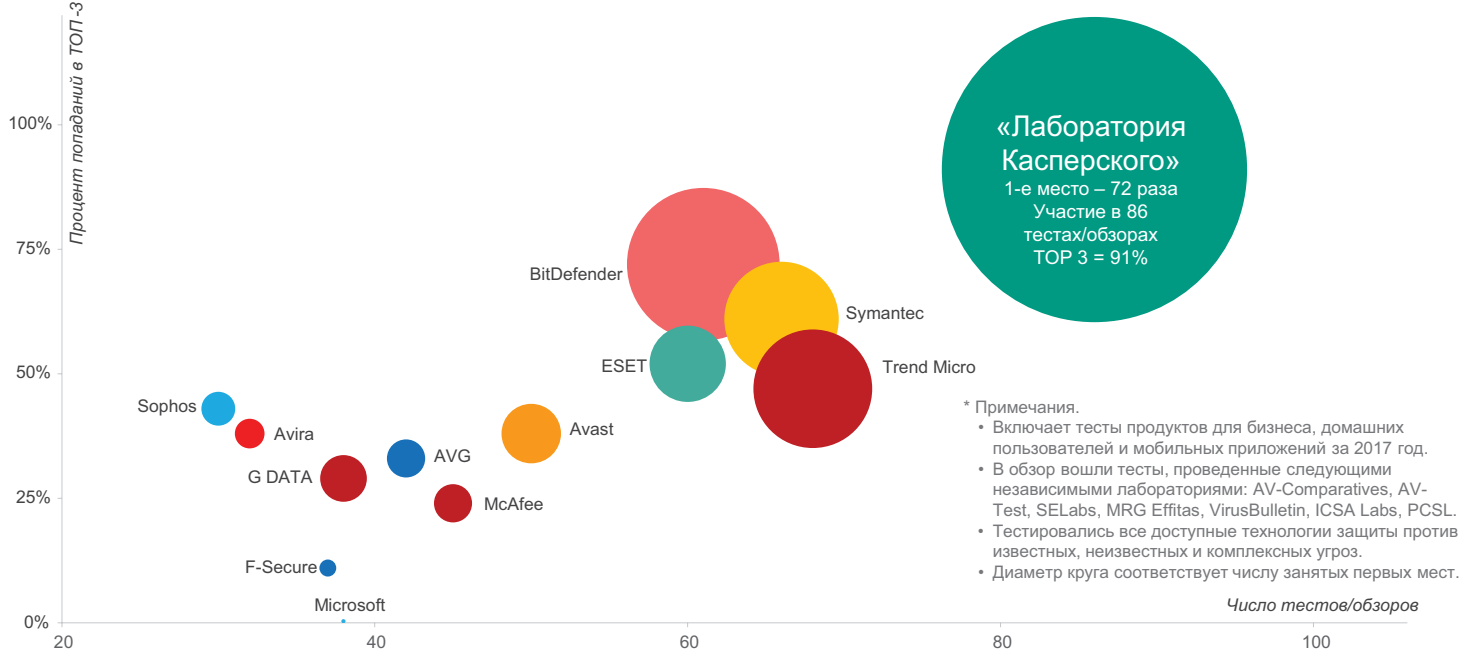
Программы повышения осведомленности

Kaspersky® Security Awareness

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

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.

Для заметок

KASPERSKY lab

АО «Лаборатория Касперского»
www.kaspersky.ru

Решения для защиты бизнеса:
www.kaspersky.ru/business

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