



**Kaspersky  
Endpoint Security  
для бизнеса**

# Защита самых ценных активов компании

Бюджеты на IT-безопасность не всегда успевают за ростом потребностей бизнеса и числа угроз. Необходимо оптимизировать ресурсы для решения текущих и будущих задач. Как выбрать подходящее решение, которое защитит все элементы IT-инфраструктуры даже от самых изощренных кибератак, обеспечит непрерывность бизнес-процессов в условиях постоянных изменений и не потребует значительного увеличения бюджета?

Наши клиенты знают ответ на этот вопрос. Kaspersky Security для бизнеса с помощью полного набора самых современных технологий обеспечивает адаптивную комплексную защиту, которая масштабируется по мере развития бизнеса и гарантирует непрерывность рабочих процессов и сохранность активов компании. Результаты говорят сами за себя.

В основе всего, что мы делаем, – самые современные средства анализа угроз. Как независимая компания мы не ограничены сложившимися шаблонами, действуем гибко и оперативно, чтобы обнаруживать и нейтрализовывать киберугрозы – вне зависимости от их целей и происхождения. За счет этого наши продукты и решения обеспечивают истинную безопасность на уровне, который не могут предложить другие разработчики.

## Истинная безопасность мирового уровня

Технологии в составе Kaspersky Endpoint Security для бизнеса обеспечивают отличный баланс между производительностью и эффективностью защиты. Именно это позволяет нашим продуктам демонстрировать высочайшие в отрасли уровни обнаружения в независимых испытаниях. «Лаборатория Касперского» вошла в тройку лучших поставщиков по данным отчета [Gartner о критических возможностях для защиты конечных устройств](#) (2018 Critical Capabilities for Endpoint Protection).

\* дается в отношении данного исследования никаких явных или подразумеваемых гарантий, включая гарантии товарной пригодности или соответствия определенным целям. Компания Kaspersky не поддерживает ни одного поставщика, продукт или услугу, которые представляются в ее исследовательских публикациях, и не рекомендует пользователям ИТ-технологий выбирать только поставщиков с наиболее высоким рейтингом. В публикациях Gartner приводятся экспертные выводы исследователей Gartner, их не следует рассматривать как факты. Компания Kaspersky не несет ответственности за содержание публикаций Gartner.

Компания Gartner не поддерживает ни одного поставщика, продукт или услугу, которые представляются в ее исследовательских публикациях, и не рекомендует пользователям ИТ-технологий выбирать только поставщиков с наиболее высоким рейтингом. В публикациях Gartner приводятся экспертные выводы исследователей Gartner, их не следует рассматривать как факты. Компания Kaspersky не несет ответственности за содержание публикаций Gartner.



- 1 **Защита серверов, шлюзов и рабочих мест**
- 2 **Оптимизация управления безопасностью через единую консоль**
- 3 **Простота и снижение совокупной стоимости владения**
- 4 **Поддержка делегирования задач участникам команды**
- 5 **Повышение производительности за счет облачных средств контроля**
- 6 **Меньше точек входа для атаки за счет круглосуточной защиты**
- 7 **Экономия времени за счет автоматизации задач развертывания ОС и ПО**



### Высокая эффективность

Наши адаптивные технологии защиты созданы мировыми экспертами, не требуют больших затрат на управление и расходуют совсем мало ресурсов. Средства защиты рабочих мест и технологии на базе машинного обучения выявляют и блокируют угрозы независимо от их происхождения и цели. А если атака все же произойдет, они откатят несанкционированные изменения, чтобы ваши сотрудники могли продолжать работу.



### Индивидуальная настройка для вашей среды

Решение защищает различные среды, легко масштабируется и требует минимального планирования даже в гетерогенных IT-инфраструктурах. Благодаря этому вы можете менять любые предустановленные настройки и добавлять новые функции в удобное вам время.



### Ведущие позиции в независимых тестированиях

Один продукт с понятным ценообразованием и лицензированием защищает все ваши данные, где бы они ни находились. Высокую удовлетворенность результатом подтверждают и наши заказчики, и независимые исследования. Ежегодно мы участвуем и побеждаем в большом количестве тестирований ([ТОП-3](#)).

# Больше чем защита рабочих мест

В основе наших технологий – технологии машинного обучения, опыт экспертов и надежные источники аналитических данных об угрозах, поступающих в режиме реального времени. С их помощью вы можете защитить важные активы своей компании от новых и изощренных кибератак.

## Защита от программ-вымогателей, бесфайловых атак и краж учетных записей

Защитите рабочие места от новейших эксплойтов и обезопасьте данные и общие папки от продвинутых угроз и программ-вымогателей. **Поведенческий анализ** с механизмом защиты памяти следит за критически важными системными процессами и предотвращает утечку идентификационных данных пользователей и администраторов.

## Сокращение вероятности атак с использованием приложений

Интегрированные средства контроля позволяют задать исчерпывающий список действий и приложений, разрешенных на рабочих станциях, тем самым заметно снижая их подверженность воздействию ранее неизвестных угроз. **Адаптивный контроль аномалий** автоматически обеспечивает максимальный уровень защиты, подходящий для той или иной роли в организации. Его дополняют инструмент Контроля программ и всегда актуальная база данных проверенных приложений для белых списков.

## Обнаружение большего количества атак и вторжений, даже самых изощренных

С помощью руткитов и буткитов злоумышленники скрывают свою деятельность от решений безопасности. Технология защиты от руткитов, включенная в многоуровневое защитное решение «Лаборатории Касперского», выявляет и нейтрализует даже самые тщательно скрытые атаки. Встроенные сенсоры и возможность интеграции с решением **Kaspersky Endpoint Detection and Response** позволяют собирать и анализировать большие объемы данных без ущерба для работы пользователей.

## Управление доступом к конфиденциальным данным и устройствам записи

Наше решение ограничивает полномочия приложений в соответствии с назначенными уровнями надежности, контролируя доступ к таким ресурсам, как зашифрованные данные. **Система предотвращения вторжений на уровне хоста (HIPS)** контролирует приложения и ограничивает доступ к важным системным ресурсам и устройствам аудио- и видеозаписи, постоянно сверяясь с локальной и облачной (Kaspersky Security Network, KSN) репутационной базой данных.

## Блокировка интернет-угроз до их проникновения на рабочие места

Наши технологии защиты фильтруют трафик на шлюзах, автоматически блокируя входящие угрозы и не позволяя им проникнуть на рабочие места и серверы. Таким образом существенно снижается риск использования уязвимостей и сокращаются операционные расходы на специалистов по защите IT-систем.

## Упрощение администрирования IT-системы

Дистанционное развертывание нового стороннего ПО – это только начало. **Автоматическая система оценки уязвимостей и установки исправлений** круглосуточно анализирует эксплуатацию уязвимостей и позволяет поддерживать актуальность потенциально уязвимого ПО, освобождая время IT-администраторов для выполнения других задач.

## Предотвращение утечки данных

Встроенная технология **Microsoft BitLocker Management** обеспечивает шифрование на уровне ОС. Вы также можете защитить данные с помощью **шифрования**, сертифицированного по стандартам FIPS 140-2 и EAL2+ общих критериев оценки защищенности информационных технологий. **Контроль устройств** защищает от последствий потери данных на неодобренных или незашифрованных устройствах и от выгрузки зараженных данных с устройств.

## Безопасность мобильных устройств

Приложение Kaspersky Security для мобильных устройств защищает от специализированных угроз, нацеленных на пересылаемые данные, и пресекает попытки проникновения в инфраструктуру через уязвимости в устройствах. Вы можете использовать имеющееся у вас **EMM-решение** для развертывания и настройки средств защиты мобильных устройств, совмещая их с актуальными бизнес-процессами компании.

## Удобное управление

Единая веб-консоль обеспечивает полную видимость и контроль над всеми рабочими станциями, серверами и мобильными устройствами независимо от их расположения и состояния. Решение Kaspersky Security для бизнеса отлично масштабируется и позволяет получить доступ к лицензиям, средствам удаленного устранения неполадок и настройкам сети. Функция централизованного управления дополняется **интеграцией с Active Directory**, управлением доступом на основе ролей и встроенными панелями мониторинга.

## Повышение производительности и снижение рисков

Решение «Лаборатории Касперского» **для защиты от спама с использованием облачных технологий** обнаруживает даже самый сложный спам на любом языке без ложных срабатываний, которые могли бы помешать передаче действительно важной информации. Остановив распространение спама и снижая связанные с ним риски и затраты времени, оно высвобождает системные и человеческие ресурсы.

## Легкое и эффективное решение даже без регулярных обновлений

Наша обширная база знаний содержит более 50 ТБ данных и более 4 миллиардов хешей. Однако эти огромные объемы аналитических данных не снижают производительность и не оттягивают на себя ваши ресурсы. Уникальный облачный режим для защиты различных компонентов инфраструктуры обеспечивает оптимальный уровень безопасности при минимальном использовании ресурсов компьютеров и интернет-трафика.

Наша математическая модель анализирует более 100 000 примеров функций и использует журналы поведенческого анализа с 10 миллионами записей для обучения моделей. И все это – в формате одного легкого пакета размером всего 2 МБ, работающего на стороне клиента.

## Актуальная система и больше преимуществ с минимальными усилиями

Обновление основных продуктов, в том числе на зашифрованных компьютерах, проходит без проблем. Защита продолжает работать даже в процессе перехода на другую версию Windows. Унифицированные политики безопасности и предустановленные настройки решения Kaspersky Endpoint Security для бизнеса можно использовать в исходном варианте или менять на ваше усмотрение, а переходить на новые версии продукта можно в удобное время с сохранением всех настроек и политик.

Улучшена отказоустойчивость решения. Поставщик сервисов по модели IaaS гарантирует, что простой инфраструктуры составят не более 4 часов в год. Консоль управления позволяет развертывать решения в облачных средах Amazon и Microsoft Azure, тем самым обеспечивая полную гибкость с точки зрения управления настройками защиты и циклами обновления. Веб-консоль можно использовать вместе с традиционной консолью MMC или вместо нее.

Мы предлагаем несколько уровней **Kaspersky Security для бизнеса** с разным объемом функций для разных этапов развития вашей компании. На каждом уровне инструменты и технологии решения сбалансированы так, чтобы удовлетворить любые потребности, связанные с безопасностью вашей IT-инфраструктуры.

## Какой уровень подходит вашей компании?

Наши решения для защиты и управления подходят компаниям разной величины и с разным подходом к обеспечению IT-безопасности. Каковы бы ни были ваши потребности, **Kaspersky Security для бизнеса** станет верным решением.



### Kaspersky Total Security для бизнеса

В компаниях с развитыми ИТ-средами, в которых есть как новые, так и давно работающие системы, необходимо проводить точную настройку безопасности с учетом требований и ограничений каждой из них. Наше самое комплексное решение безопасности для рабочих мест, шлюзов и серверов позволяет это сделать. Вы получите надежную и гибкую защиту, которую можно подстроить под ваши ИТ-активы.



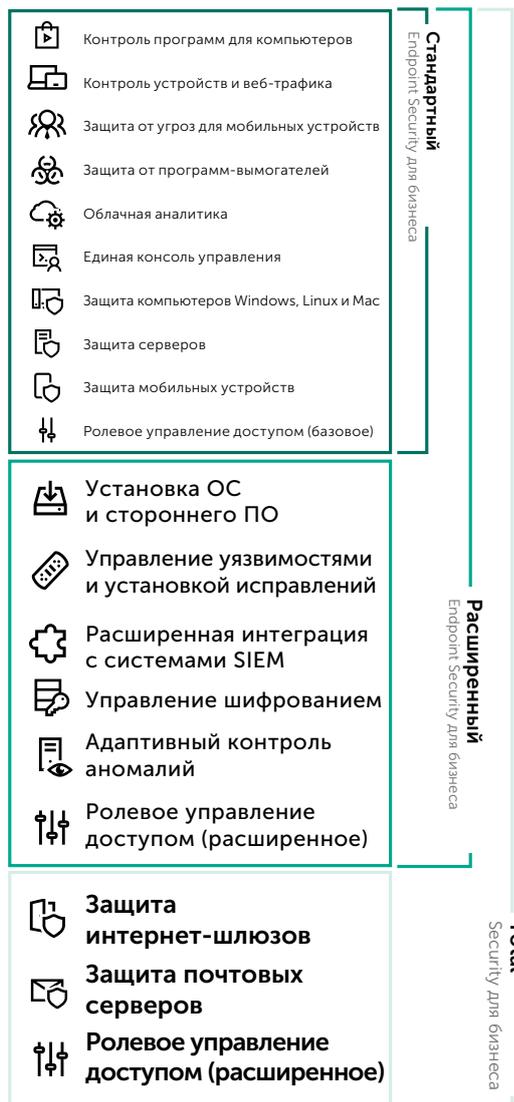
### Kaspersky Endpoint Security для бизнеса Расширенный

Если вам требуется решение безопасности, работающее в более напряженном режиме, выбирайте Kaspersky Endpoint Security для бизнеса Расширенный. Помимо защиты рабочих мест и серверов, это решение содержит инструменты патч-менеджменты, встроенное шифрование, а также помогает оптимизировать процессы управления безопасностью систем.



### Kaspersky Endpoint Security для бизнеса Стандартный

Все больше коммерческих операций выполняется в электронной форме, поэтому необходимо следить за безопасностью каждого сервера с Linux, ноутбука Mac и мобильного устройства с Android. Мы предлагаем гибкий подход к безопасности, который поможет защитить все конечные устройства в компании с помощью одного решения с единой гибкой консолью управления.





В 2018 году «Лаборатория Касперского» была признана победительницей в рейтинге **Gartner Peer Insights Customers' Choice** в категории **платформ для защиты конечных устройств (EPP)** – и уже не в первый раз. В 2017 году, когда награда впервые вручалась в этой категории, «Лаборатория Касперского» стала единственным поставщиком, удостоившимся ее высшего, **платинового** уровня. Мы гордимся столь высокой оценкой самых уважаемых судей – наших клиентов. В 2018 году наш итоговый рейтинг составил 4,7 из 5 баллов.

#### Открытость и соответствия требованиям

Для компаний важна непредвзятость и неприкосновенность коммерческих данных. Наши продукты только обрабатывают, но никогда не собирают их. Статистическая информация обрабатывается в Швейцарии, чтобы гарантировать нейтралитет с геополитической точки зрения. На пути к полной открытости наша компания сделала важный шаг – организовала первый в отрасли центр прозрачности. Надеемся, что нашему примеру последуют и другие поставщики.

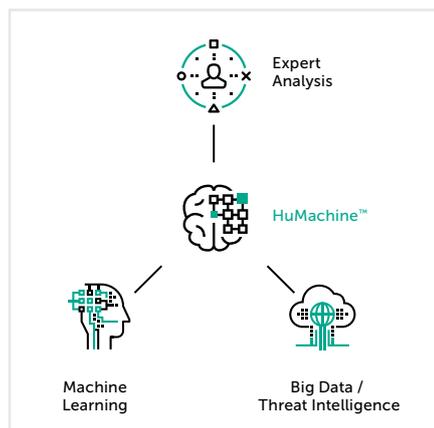
## Поддержка и дополнительные услуги

«Лаборатория Касперского» обеспечивает техническую поддержку более чем в 200 странах из 35 офисов по всему миру. Помощь доступна ежедневно и круглосуточно. Наши обязательства по поддержке на глобальном уровне отражены в соглашении о сервисном обслуживании (MSA). Наши отделы профессиональных сервисов готовы в любой момент помочь с развертыванием и при возникновении критических инцидентов, чтобы вы получали максимальную отдачу от вашего защитного решения.

## Признание заказчиков

Те, кто уже перешел на Kaspersky Security для бизнеса и пользуется преимуществами этого решения, отмечают следующие преимущества этого решения:

- Постоянно высокий уровень защиты. Простой одноэтапный переход на новые версии помогает поддерживать систему в актуальном состоянии и отражать самые современные кибератаки.
- Удобный интерфейс и централизованное управление. Один сервер, одна веб-консоль, один агент.
- Глубокая интеграция компонентов. Все компоненты связаны между собой, что упрощает работу администраторов.
- Все нужные функции сразу, в рамках одной покупки. Прозрачное ценообразование и лицензирование.



[www.kaspersky.ru](http://www.kaspersky.ru)

#ИстиннаяБезопасность

© АО «Лаборатория Касперского», 2019. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.