Решения для защиты бизнеса

KASPERSKY lab

Kaspersky Security для бизнеса. Новое поколение защиты корпоративной сети

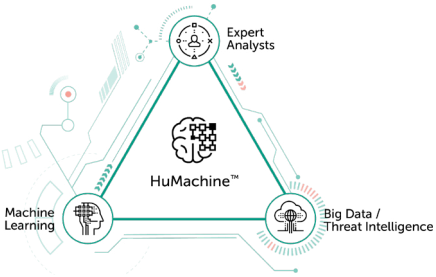
www.kaspersky.ru/business
#истиннаябезопасность

Kaspersky ®
Security
для бизнеса

Стратегическое решение для обеспечения непрерывности бизнеса

Технологии стимулируют развитие бизнеса и помогают ему идти в ногу со временем. Однако у технологий есть и обратная сторона – кибератаки. По-прежнему сильнее всего от них страдают конечные устройства. Только за последний год более 38% компаний подверглись кибератакам, и 39% атак на защищенные рабочие станции увенчались успехом. Для успешной борьбы с угрозами компании должны быть умнее и дальновиднее, чем те, кто их атакует.

Пока за кибератаками стоят люди, им сможет противостоять человеческий интеллект в сочетании с инновационными технологиями. Защита «Лаборатории Касперского» работает на основе наших глобальных аналитических данных об угрозах, подкрепленных алгоритмами машинного обучения и опытом лучших экспертов в области кибербезопасности. Это уникальное сочетание, которое мы назвали HuMachine™, является отличительной особенностью наших продуктов



В 2017 году «Лаборатория Касперского» была отмечена платиновой наградой **Gartner Peer Insights в категории «Платформы для защиты рабочих мест» (Endpoint Protection Platforms)**. Эта награда представляет собой наивысшую степень признания на конкурентном рынке платформ защиты рабочих мест.

Защита как инвестиция в будущее

Средний размер ущерба в результате одного инцидента ИБ для компаний среднего бизнеса составляет 1,6 млн. рублей, а для крупного бизнеса он в десять раз выше – 16,1 млн. рублей.* Современной антивирусной программы уже недостаточно – необходимо комплексное решение, отвечающее за безопасность на нескольких технологических и функциональных уровнях корпоративной IT-инфраструктуры. Истинная защита рабочих мест сочетает в себе различные интеллектуальные методы и технологии для защиты от любых киберугроз на любой платформе. Обезопасив всю корпоративную IT-сеть, вы сможете обеспечить непрерывность бизнеса.

Передовые технологии, удобное управление

Бюджет информационной безопасности не может расти с той же скоростью, что и компания. Защитные решения должны обеспечивать безопасность от самых сложных угроз – текущих и будущих. Решение Kaspersky Security для бизнеса, использующее передовые технологии машинного обучения, защищает от программ-шифровальщиков, эксплойтов и самых опасных атак. Это современное решение оснащено удобными и гибкими средствами настройки защиты, автоматизированной системой оценки уязвимостей и установки исправлений, а также встроенными функциями шифрования**. Всю корпоративную сеть можно контролировать из единой консоли.

Гибкость

Решение рассчитано на работу в любой IT-среде и просто масштабируется, если требования к защите растут. Встроенные сенсоры и возможность интеграции с решением Kaspersky Endpoint Detection and Response позволяют анализировать большие объемы данных для обнаружения скрытых кибератак.

Высокая производительность

Решение оптимально защищает устройства на всех популярных платформах, минимально влияя на их производительность. Компоненты, не полагающиеся в работе на сигнатуры, способны выявлять угрозы даже без частого обновления.

Защита важных данных

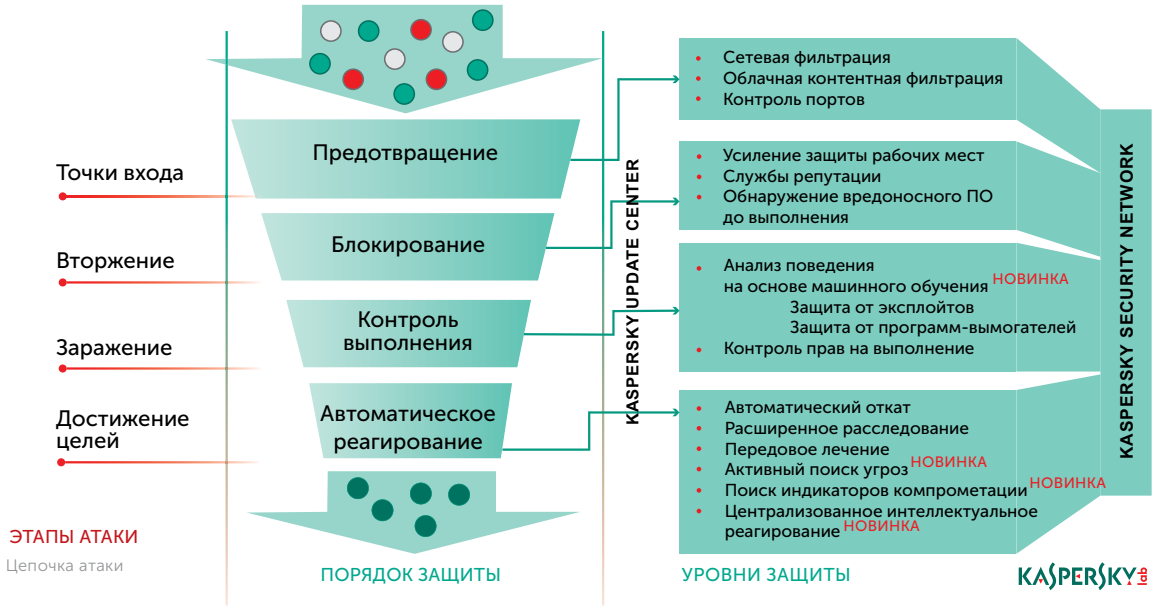
Решение защищает компанию и сотрудников от целого ряда угроз, нацеленных на похищение или нарушение целостности данных, в том числе с помощью встроенного шифрования и контейнеризации корпоративных данных на мобильных устройствах.

*Глобальное исследование рисков информационной безопасности, «Лаборатория Касперского», 2017

**Начиная с уровня Kaspersky Endpoint Security для бизнеса Расширенный

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 защита от эксплойтов. Они нейтрализуют большинство угроз еще до срабатывания передовых уровней защиты. Подозрительные файлы, достигающие рабочих станций, обнаруживаются и блокируются.



Несколько уровней защиты для:

- компьютеров Windows, Linux или Mac;
- устройств Android и других мобильных устройств;
- съемных носителей;
- серверов Windows и Linux;
- почтовых серверов;
- интернет-шлюзов;
- серверов совместной работы.

Надежная защита от:

- эксплойтов;
- программ-вымогателей;
- вредоносных программ для мобильных устройств;
- неизвестных угроз;
- бесфайловых атак;
- скриптов PowerShell и других атак на основе скриптов;
- интернет-угроз;
- угроз, распространяемых по электронной почте;
- фишинговых атак;
- спама.

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. Контроль приложений отслеживает запуск исполняемых файлов и библиотек DLL и контролирует скрипты, выполняемые различными интерпретаторами. Поведенческий анализ и Защита от эксплойтов отслеживают поведение программ, блокируют потенциально опасную активность и защищают надежные приложения от эксплуатации и поражения вредоносными программами. Проверенные и надежные приложения смогут работать бесперебойно.

Нейтрализация руткитов

С помощью руткитов и буткитов злоумышленники скрывают свою деятельность. Технология защиты от руткитов, включенная в решение, выявляет и нейтрализует даже самые тщательно скрытые инфекции.

Обнаружение даже самых сложных атак

Встроенные сенсоры и возможность интеграции с решением Kaspersky Endpoint Detection and Response позволяют собирать и анализировать большие объемы данных без ущерба для производительности труда пользователей. Среди этих данных осуществляется расширенный поиск угроз по свидетельствам взлома, таким как индикаторы компрометации (IoC).

Предотвращение доступа через сеть

Вредоносные программы, использующие атаки с переполнением буфера, могут изменять запущенный в памяти процесс и выполнять свой вредоносный код. Защита от сетевых угроз обнаруживает сетевые атаки и эксплойты, останавливая их продвижение.

Обслуживание и поддержка

«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 защитного решения «Лаборатории Касперского».

Пробная версия

Чтобы самостоятельно оценить качество защиты и удобство управления, вы можете получить бесплатную 30-дневную полнофункциональную версию решения **Kaspersky Security для бизнеса**. Если в конце пробного периода вы решите приобрести продукт, вам потребуется только оплатить стоимость лицензии, никаких дополнительных установок и настроек производить не потребуется.

Не только защита от вредоносного ПО — передовые технологии для безопасности вашей компании

Упрощение инвентаризации и установки исправлений

Сбор информации о программном и аппаратном обеспечении и своевременная установка исправлений отнимают много времени и сил. С помощью расширенных инструментов системного администрирования вы видите, какое ПО нужно обновлять как можно скорее, и можете распространить обновления удаленно, в том числе в нерабочее время. Кроме того, вы всегда можете контролировать устройства и программы в вашей корпоративной сети.

Безопасный совместный доступ к данным с шифрованием

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.

Поддержка сценариев использования удаленных и мобильных устройств

Технологии обеспечения безопасности мобильных устройств защищают от угроз пересылаемые данные и пресекают попытки проникновения в инфраструктуру через уязвимости в устройствах. Контроль устройств защищает от последствий потери данных на неодобренных или незашифрованных устройствах и от выгрузки зараженных данных с устройств.

Повышение эффективности с помощью 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.

Управление доступом к конфиденциальным данным и устройствам записи

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

Блокирование интернет-угроз

Останавливая большую часть входящих угроз на уровне шлюза, решение существенно снижает влияние человеческого фактора и особенностей защиты рабочих станций на проникновение угроз.

Защищенный шлюз продолжает служить первой линией обороны в большинстве сценариев угроз корпоративной безопасности, несмотря на включение мобильных устройств в рабочие процессы. Наши технологии защиты осуществляют фильтрацию трафика, проходящего через шлюзы, 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.

Kaspersky Endpoint Security для бизнеса предоставляет администраторам возможности для мониторинга, контроля и защиты IT-инфраструктуры. Сбалансированные на разных уровнях инструменты и технологии нового поколения вместе способны удовлетворить любые потребности, связанные с безопасностью IT-инфраструктуры на каждом этапе развития компании.

Kaspersky® Total Security для бизнеса

Наиболее комплексное решение, которое содержит защиту не только рабочих мест, но и других, потенциально уязвимых узлов – серверов совместной работы, 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

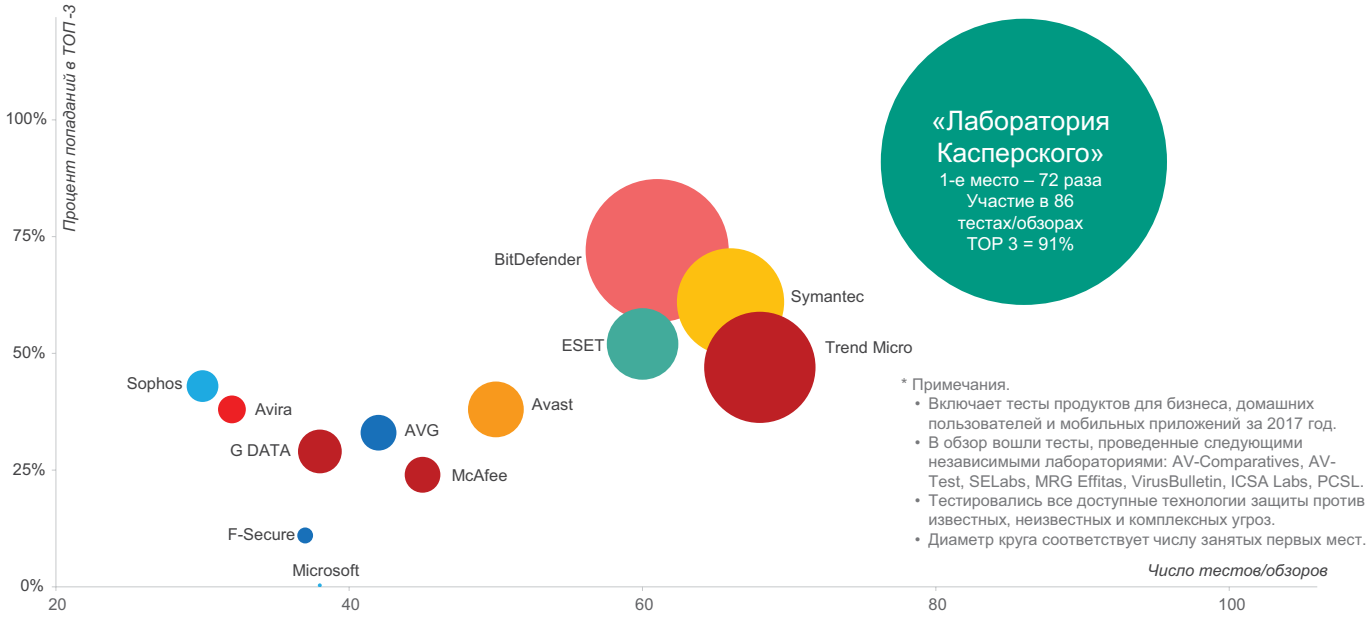
Решение нового поколения, которое поможет защитить все используемые компанией рабочие места с помощью одного продукта с гибкой консолью управления.

Какой уровень подходит вам?

Каковы бы ни были ваши потребности, связанные с безопасностью IT-инфраструктуры, **Kaspersky Security для бизнеса** станет оптимальным решением.

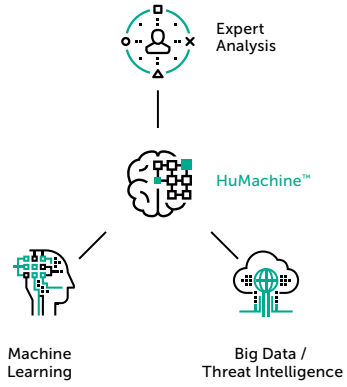
Больше тестов. Больше наград. Больше защиты*

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).



Узнайте больше о продуктах «Лаборатории Касперского»

Защита рабочих мест – это только часть системы обеспечения безопасности. «Лаборатория Касперского» предлагает широкий набор продуктов, которые предназначены для защиты отдельных узлов сети и дополняют Kaspersky Security для бизнеса. Узнайте больше о продуктах «Лаборатории Касперского» для среднего бизнеса на сайте: kaspersky.ru/business.



«Лаборатория Касперского»

www.kaspersky.ru

#истиннаябезопасность
#HuMachine

KESB_Product_Datasheet_Next_Generation_Endpoint_Protection_Customer_0218_EN_GLB