Kaspersky Security для бизнеса

Линейка решений Kaspersky Security для бизнеса обеспечивает комплексную многоуровневую защиту корпоративной сети от известных, неизвестных и сложных угроз. Уникальное сочетание аналитических данных, технологий машинного обучения и опыта экспертов позволяет успешно бороться с угрозами любого типа и масштаба.

Подробнее на kaspersky.ru/business

Kaspersky® Security для бизнеса

Kaspersky Endpoint Security для бизнеса Стандартный

Защита от киберугроз для компаний любой величины

Kaspersky Endpoint Security для бизнеса Стандартный — удобное в управлении и легко масштабируемое решение, обеспечивающее мощную многоуровневую защиту от актуальных киберугроз. Средства контроля использования программ, устройств и веб-ресурсов помогают гибко управлять системой безопасности компании, а инструменты управления мобильными устройствами и приложениями позволяют повысить эффективность работы сотрудников без риска потери данных.

Защита от актуальных киберугроз для бизнеса

Оперативная и надежная защита

Истинная безопасность возможна, когда технологии и средства защиты готовы отразить любую возможную кибератаку. Решения «Лаборатории Касперского» для защиты бизнеса объединяют опыт экспертов, анализ «больших данных» об угрозах и возможности машинного обучения. Возникающее в результате взаимодействие между людьми и машинами — HuMachine™ —позволяет справляться со всеми видами атак, направленными против компаний.

Проактивная борьба с угрозами

В Kaspersky Endpoint Security для бизнеса Стандартный признанные средства обнаружения и блокирования вредоносного ПО дополнены многими дополнительными уровнями защиты. Так Мониторинг системы выявляет и блокирует подозрительные действия, указывающие на возможную активность программы-шифровальщика, а система предотвращения вторжений (HIPS) с персональным сетевым экраном помогает контролировать приложения и сетевую активность.

Широкие возможности контроля и управления

Контроль программ

Контроль программ с динамическими белыми списками позволяет IT-администраторам разрешать, блокировать и регулировать использование программ. Одним из самых эффективных способов обеспечения безопасности является режим «Запрет по умолчанию», который запрещает использование любых программ за исключением разрешенных. Контроль привилегий позволяет ограничивать права доступа программ к выбранным файлам и ресурсам.

Веб-Контроль

Инструменты веб-контроля, предлагаемые «Лабораторией Касперского», позволяют создавать политики доступа в интернет и контролировать его при помощи широкого набора готовых и настраиваемых категорий. Инструменты контроля можно интегрировать с Active Directory для более гибкой настройки политик.

Контроль устройств

Kaspersky Security для бизнеса позволяет создавать политики, регулирующие подключение съемных носителей и других периферийных устройств. Также возможен контроль доступа программ к устройствам аудио- и видеозаписи. Кроме того, решение Kaspersky Security для бизнеса регистрирует все операции удаления и копирования, выполненные на съемных USB-устройствах, и управляет правами пользователей в отношении операций чтения и записи файлов на CD- и DVD-диски.

Защита файловых серверов

Надежная защита от вредоносного ПО и шифровальщиков

Управление защитой файловых серверов выполняется вместе с управлением защитой устройств через Kaspersky Security Center. Обеспечена поддержка всех основных серверных платформ с минимальным воздействием на производительность.

Безопасность мобильных устройств

Многоуровневая защита и контроль мобильных устройств

Защиту мобильных устройств обеспечивают проактивные, облачные и другие передовые методы. Корпоративные данные и приложения находятся в контейнерах — таким образом, они размещены независимо от личных приложений пользователя и их можно дополнительно защитить паролем. Функция Анти-Вор помогает обезопасить данные в случае потери или кражи устройства — например, администратор может удаленно стереть все корпоративные данные.

Гибкое управление защитой

Централизация управления и контроля

Управление Kaspersky Security для бизнеса осуществляется из единой консоли Kaspersky Security Center, которая обеспечивает централизованный контроль настроек безопасности для каждого устройства в сети. Средства администрирования и управления интуитивно понятны и эффективны. Администраторы могут создавать политики в соответствии с конкретными требованиями или использовать готовые политики. Контроль доступа на основе ролей позволяет распределять обязанности администраторов в сложных сетях.

Kaspersky Endpoint Security для бизнеса Расширенный

Расширенные средства управления и защиты данных

Kaspersky Endpoint Security для бизнеса Расширенный сочетает многоуровневую защиту от угроз с широкими возможностями управления и защиты корпоративных данных. Это выбор компаний, которые уделяют пристальное внимание защите конфиденциальной информации и стремятся защитить сложную корпоративную среду от атак нулевого дня. Кроме того, это решение позволяет IT-департаменту оперативнее и эффективнее выполнять многие повседневные задачи, что сокращает расходы и позволяет высвободить ресурсы, необходимые для развития IT-инфраструктуры.

Защита от эксплойтов и атак нулевого дня

Автоматический поиск уязвимостей и установка исправлений

Автоматизированное выявление и приоритизация уязвимостей ОС и приложений, в сочетании с быстрым автоматическим распространением исправлений и обновлений, повышает надежность защиты, в то же время обеспечивая более эффективное администрирование и уменьшая сложность управления IT-инфраструктурой. Автоматизированная проверка программ позволяет быстро обнаруживать их устаревшие версии, нарушающие безопасность и требующие обновления.

Эффективное управление IT-системами

Удаленное устранение неполадок

Доступно удаленное развертывание и установка программ по требованию и по расписанию, включая поддержку технологии Wake-on-LAN. Удаленное устранение неполадок и эффективное распространение ПО выполняется при помощи технологии Multicast.

Простое развертывание ОС

Решение позволяет легко создавать, хранить и развертывать «золотые образы» операционной системы при помощи консоли управления и поддерживает интерфейс UEFI.

Мониторинг в режиме реального времени

Благодаря интеграции с SIEM-системами, такими как IBM® QRadar® и HP® ArcSight®, компании могут получать полную информацию о безопасности корпоративной сети в режиме реального времени.

Защита конфиденциальных данных

Шифрование данных

Технологии полного шифрования диска (FDE) и шифрования файлов (FLE) для безопасной передачи данных доступа обеспечивают безопасность корпоративных данных в сети. В целях повышения безопасности сразу после шифрования файла исходные незашифрованные данные можно удалять с жесткого диска. Также доступно шифрование в портативном режиме и шифрование съемных носителей.

Гибкая процедура входа в систему	Аутентификация перед загрузкой допускает однократную авторизацию для удобства пользователей (шифрование происходит для них незаметно). Кроме того, возможна двухфакторная аутентификация при помощи смарт-карт и токенов.
Интеграция с инструментами контроля	Уникальная интеграция средств шифрования с инструментами контроля приложений и устройств создает дополнительный слой защиты и упрощает администрирование.
Улучшенная совместимость с аппаратным обеспечением	Шифрование жесткого диска на устройствах под управлением Microsoft® Windows® можно выполнять при помощи технологии Microsoft BitLocker®. Microsoft BitLocker — это средство шифрования, встроенное в Microsoft Windows. Оно позволяет улучшить совместимость с аппаратным обеспечением и сводит к минимуму неудобства для пользователя.

На уровне Расширенный доступны все компоненты уровня Стандартный.

Kaspersky Total Security для бизнеса

Комплексная IT-безопасность на различных уровнях сети

Kaspersky Total Security для бизнеса обеспечивает максимальную безопасность для компаний всех размеров. Мощные инструменты контроля и расширенные возможности системного администрирования дополнены защитой второго контура — почтовых серверов, интернет-шлюзов и платформ совместной работы. Это решение способно защитить самые сложные корпоративные среды с исключительно высокими требованиями к безопасности.

Комплексная защита почтовых серверов

Решение поддерживает широкий ряд типов почтовых серверов, защищая почтовый трафик от вредоносных программ и спама. Облачные обновления в режиме реального времени обеспечивают высочайший уровень обнаружения и минимальное количество ложных срабатываний. На базе Kaspersky Total Security для бизнеса также можно настроить выделенный почтовый шлюз. Отдельно доступны технологии защиты от утечки данных — Kaspersky DLP для Microsoft Exchange Servers.

Защита интернет-шлюзов

Решение обеспечивает защиту трафика, проходящего через наиболее распространенные шлюзы на базе Windows и Linux®: оно автоматически удаляет вредоносные и потенциально опасные программы из трафика на основе протоколов HTTP, HTTPS, FTP, SMTP и POP3.

Защита платформ совместной работы

Средства совместной работы повышают продуктивность, но, как и все остальное, требуют защиты. Для платформ SharePoint доступна защита от вредоносного ПО, контентная фильтрация и фильтрация файлов. Эти технологии помогают компаниям применять политики совместной работы и исключают хранение нежелательного содержимого в корпоративной сети. В качестве дополнительной возможности защиты платформ совместной работы доступны технологии Kaspersky DLP.

На уровне Total доступны все компоненты уровней Стандартный и Расширенный.

Истинная безопасность — цель всей нашей деятельности

«Лаборатория Касперского» предлагает передовые средства защиты от вредоносных программ, которые опираются на признанную в мире глубокую и всестороннюю аналитику угроз. Это отличительная особенность нашей компании, которая проявляется во всех аспектах нашей деятельности. Будучи независимой компанией, мы можем думать нестандартно, проявлять большую гибкость и действовать быстрее.

- **Развитие технологий — наш приоритет:** мы разрабатываем все свои основные технологии внутри компании, благодаря чему наши продукты более стабильны и эффективны. Мы уделяем максимальное внимание исследованиям и разработкам.

- **Глобальный центр исследования и анализа угроз (GReAT)** задает направление всей работе «Лаборатории Касперского», занимая ведущие позиции в анализе угроз и расследовании инцидентов кибербезопасности. Это подразделение экспертов по IT-безопасности обнаружило многие из самых опасных в мире вредоносных программ и целевых атак.

- «Лаборатория Касперского» **является доверенным партнером международных организаций** по борьбе с киберпреступностью, включая Интерпол и Европол.

- **Решения «Лаборатории Касперского» завоевали рекордное число первых мест** в независимых тестах и обзорах. Подробнее — на kasperksy.ru/top3.

- Мы защищаем свыше **400 миллионов пользователей в 140 странах мира**. Каждый год пользователи активируют активируют продукты «Лаборатории Касперского» 20 миллионов раз.

- Ведущие отраслевые аналитики — в том числе Gartner, Inc., Forrester Research и International Data Corporation (IDC) — признают «Лабораторию Касперского» лидером во многих ключевых областях IT-безопасности. **В 2017 году компания в шестой раз подряд заняла место в категории «Лидеры» Магического квадранта Gartner.**

- **Наши технологии защиты используют ведущие мировые поставщики** IT-решений: Microsoft, Cisco®, Juniper®, TrustWave® и многие другие.

www.kaspersky.ru
#ИстиннаяБезопасность

Как приобрести

Чтобы выбрать нужный вам продукт из линейки Kaspersky Security для бизнеса, проконсультируйтесь с партнером «Лаборатории Касперского». Контактная информация и адреса партнеров представлены на нашем сайте в разделе www.kaspersky.ru/find_partner_office