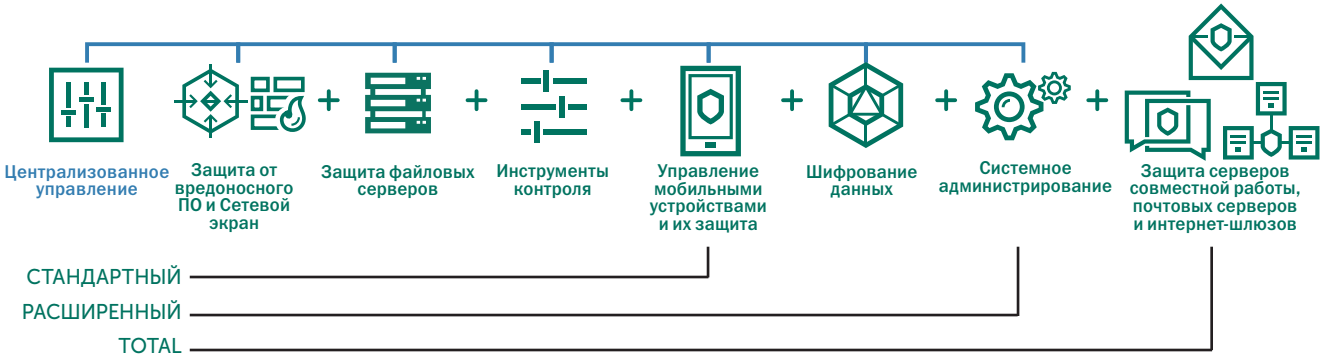
KASPERSKY SECURITY ДЛЯ БИЗНЕСА

Многоуровневая защита IT-инфраструктуры от всех видов киберугроз

Kaspersky Security для бизнеса — это комплексное защитное решение, разработанное ведущими мировыми экспертами в области IT-безопасности. С помощью Kaspersky Security для бизнеса администраторы могут централизованно контролировать и защищать корпоративную IT-инфраструктуру. Оптимальным образом подобранные инструменты и технологии формируют несколько уровней решения с нарастающим функционалом. Надежная защита, действующая на опережение, высокая производительность и удобное централизованное управление позволяют обеспечить IT-безопасность вашего бизнеса.

Все компоненты разработаны внутри компании на собственной технологической базе и составляют единую платформу для обеспечения безопасности, легко адаптируемую в соответствии с потребностями вашего бизнеса. В результате вы получаете стабильное интегрированное решение без брешей в защите и проблем совместимости, не перегружающее ресурсы вашей IT-инфраструктуры.



KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА СТАНДАРТНЫЙ

Мощные и гибкие инструменты защиты от вредоносного ПО, контроля рабочих мест и обеспечения безопасности мобильных устройств.

Высокоэффективное решение для защиты от вредоносных программ с возможностями централизованного развертывания и управления, а также формирования отчетов — основа платформы для обеспечения IT-безопасности корпоративной сети.

Инструменты Веб-Контроля и Контроля устройств и приложений, с поддержкой регулярно обновляемых динамических белых списков, обеспечивают дополнительный уровень защиты рабочих мест.

Корпоративные мобильные устройства и личные устройства сотрудников, используемые в рабочих целях (BYOD), также надежно защищены от актуальных угроз. Безопасностью всех рабочих мест можно управлять с помощью единой консоли Kaspersky Security Center. Защита файловых серверов предотвращает распространение зараженных файлов по локальной сети

ЗАЩИТА РАБОЧИХ МЕСТ ОТ ВРЕДОНОСНОГО ПО

Защита от известных, неизвестных и сложных угроз — передовые технологии «Лаборатории Касперского» позволяют выявлять и эффективно устранять уже существующие и новые угрозы.

Автоматическая защита от эксплойтов — проактивно выявляет и блокирует неизвестные и сложные угрозы.

Защита из облака – обеспечивает IT-безопасность с использованием информации, поступающей в режиме реального времени из глобальной облачной репутационной базы данных об угрозах Kaspersky Security Network.

Мониторинг активности — включает уникальную функцию восстановления файлов в случае заражения системы с помощью инструмента Откат вредоносных действий.

Система предотвращения вторжений и персональный Сетевой экран — ограничивают действия приложений и их сетевую активность на рабочих местах в зависимости от степени доверия, присвоенной каждому приложению.

КОНТРОЛЬ РАБОЧИХ МЕСТ

Контроль программ и динамические белые списки — сведения о репутации файлов, поступающие из облачной репутационной базы данных об угрозах Kaspersky Security Network в режиме реального времени, позволяют системным администраторам разрешать, блокировать или ограничивать использование приложений, а также применять политику «запрета по умолчанию» на основе белых списков в реальной или тестовой среде. Инструменты контроля активности программ и мониторинга уязвимостей наблюдают за работой приложений и ограничивают действия тех из них, чье поведение является подозрительным.

Веб-Контроль – политики использования веб-ресурсов могут создаваться на базе предварительно установленных или настраиваемых категорий, обеспечивая всесторонний контроль и высокую эффективность администрирования.

Контроль устройств – позволяет создать, запланировать и внедрить гибкие политики работы с данными, контролирующие подключение съемных носителей и других периферийных устройств, в том числе с использованием масок — для одновременного развертывания политик на многих устройствах.

ЗАЩИТА ФАЙЛОВЫХ СЕРВЕРОВ

Защита от шифрования — препятствует попыткам программ-вымогателей зашифровать данные на файловых серверах с целью получению выкупа.

Сохранение непрерывности бизнеса — всесторонняя защита сервера от вредоносных программ, которая блокирует даже новейшие и потенциальные угрозы. Это позволяет свести к минимуму перебои в рабочих процессах предприятия, вызванные вредоносным ПО, а также уменьшить связанные с ними затраты.

Мощная система отчетности и управления — удобные, интуитивно понятные инструменты управления, сведения о статусе защиты серверов, гибкие настройки времени сканирования и система подробных отчетов обеспечивают эффективный контроль безопасности файловых серверов, что помогает сократить расходы на их содержание.

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ

Мощная защита мобильных устройств — сочетание сигнатурных, проактивных и облачных технологий для обеспечения многоуровневой защиты мобильных рабочих мест в режиме реального времени. Компоненты Веб-Контроль, Анти-Спам и Антифишинг обеспечивают дополнительный уровень безопасности устройств.

Защита данных в случае потери или кражи устройства — компонент Анти-Вор предоставляет возможность удаленно заблокировать потерянное устройство, удалить с него данные (полностью или выборочно), определить местонахождение, узнать новый номер устройства в случае замены в нем SIM-карты, включить на устройстве звуковой сигнал (сирену), а также незаметно сфотографировать нового «владельца». Все эти функции позволяют предотвратить доступ посторонних лиц к корпоративным данным в случае кражи или утери мобильного устройства.

Управление мобильными приложениями (MAM) — допускает использование сотрудником приложений только из белого списка, предотвращая установку нежелательного или неизвестного ПО. Технология контейнеризации позволяет изолировать корпоративные данные на личных устройствах сотрудников. К информации, помещенной в контейнеры, могут удаленно применяться функции шифрования или выборочной очистки.

Управление мобильными устройствами (MDM) — позволяет применять групповые политики безопасности ко всем устройствам или группе устройств. Кроме того, благодаря гибким настройкам, администраторы могут зашифровать отдельное устройство, запретить ему доступ к определенным приложениям, узнать информацию об устройстве и т. п. Развертывание политик осуществляется с помощью SMS, электронных писем или через компьютеры.

KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА РАСШИРЕННЫЙ

В дополнение к инструментам уровня СТАНДАРТНЫЙ средства системного администрирования повышают эффективность защиты и производительность IT-инфраструктуры, а интегрированная функция шифрования защищает конфиденциальные данные.

Автоматическая установка исправлений и управление образами ОС, удаленное распространение ПО и интеграция с SIEM-системами — все это помогает упростить администрирование, а учет аппаратного и программного обеспечения и контроль управления лицензиями обеспечивают эффективный мониторинг и всесторонний контроль корпоративных IT-ресурсов. Встроенная технология шифрования предоставляет дополнительный уровень защиты данных. Безопасность файловых серверов, в дополнение к средствам защиты уровня СТАНДАРТНЫЙ, усилена Контролем запуска приложений.

СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Мониторинг уязвимостей и установка исправлений — автоматическое выявление и приоритизация уязвимостей в ОС и приложениях в сочетании с быстрым автоматическим распространением исправлений и обновлений.

Развертывание ОС и программ — простое централизованное создание и развертывание эталонных образов ОС и их компонентов с поддержкой интерфейса UEFI.

Распространение ПО и устранение неполадок — удаленное развертывание ПО, а также обновлений ОС и приложений, по запросу или по расписанию, в том числе с использованием Wake-on-LAN. Технология Multicast позволяет экономить время IT-администраторов, обеспечивая удаленное устранение неполадок и распространение ПО.

Учет аппаратного и программного обеспечения и управление лицензиями — идентификация, мониторинг и контроль (включая блокирование), а также исчерпывающая информация об использовании лицензий позволяют администраторам эффективно управлять всем аппаратным и программным обеспечением, установленным в корпоративной сети, включая съемные носители.

Интеграция с SIEM-системами — поддержка систем IBM® QRadar® и HP® ArcSight®.

Разделение прав администраторов на основе ролей — в сложных сетях обязанности IT-администраторов могут быть распределены в соответствии с назначенными ролями. Администраторам с разными правами доступны разные компоненты консоли управления.

ШИФРОВАНИЕ

Надежная защита данных — на рабочих местах могут применяться как шифрование на уровне файлов/папок (FLE), так и полнодисковое шифрование (FDE). Специальный режим для портативных устройств позволяет применить шифрование, когда такие устройства покидают периметр корпоративной сети.

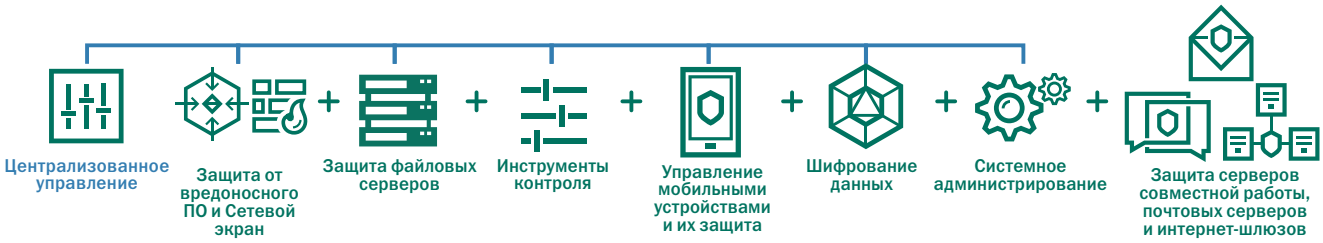
Гибкий подход к авторизации — для повышения уровня безопасности предусмотрена возможность однократной авторизации перед загрузкой системы, что позволяет обеспечить максимальную прозрачность для пользователя. Также поддерживается двухфакторная аутентификация посредством токенов.

Интегрированные политики — уникальная интеграция политик шифрования с функционалом контроля устройств и программ обеспечивает дополнительный уровень защиты и упрощает администрирование.

ЗАЩИТА ФАЙЛОВЫХ СЕРВЕРОВ

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.

KASPERSKY TOTAL SECURITY ДЛЯ БИЗНЕСА



Идеальное решение для организаций с высокими требованиями к IT-безопасности, которым нужна надежная защита каждого узла сети. Сочетает в себе функции предыдущих уровней с возможностями защиты серверов совместной работы, почтовых серверов интернет-шлюзов.

Kaspersky Total Security для бизнеса — наиболее полнофункциональное решение для защиты и управления корпоративной IT-инфраструктурой из представленных сегодня на рынке. Kaspersky Total Security для бизнеса защищает вашу корпоративную сеть на всех уровнях и включает мощные инструменты настройки, позволяющие обеспечить продуктивную работу пользователей, а также надежную защиту от любых интернет-угроз — независимо от местонахождения сотрудников организации и используемых ими устройств.

ЗАЩИТА ПОЧТОВЫХ СЕРВЕРОВ

Эффективно защищает от распространяемых через электронную почту вредоносных программ, фишинговых атак и спама, используя обновления из облака в режиме реального времени, что позволяет добиться высочайшего уровня обнаружения при минимальном количестве ложных срабатываний. Поддерживает платформы Microsoft® Exchange Server, Linux® Mail Server и IBM® Lotus Domino®. Для серверов Microsoft Exchange отдельно доступен функционал контроля над распространением конфиденциальной информации — Kaspersky DLP.

ЗАЩИТА ИНТЕРНЕТ-ШЛЮЗОВ

Обеспечивает безопасный доступ в интернет для всех сотрудников организации благодаря автоматическому удалению вредоносных и потенциально опасных программ из трафика HTTP(S) и FTP.

ЗАЩИТА СЕРВЕРОВ СОВМЕСТНОЙ РАБОТЫ

Защищает серверы и фермы серверов Microsoft SharePoint® от всех типов вредоносного ПО. Доступный отдельно функционал контроля над распространением конфиденциальной информации – Kaspersky DLP для серверов SharePoint – отвечает за фильтрацию контента и файлов, позволяет эффективно выявлять конфиденциальную информацию и обеспечивает надежную защиту от утечки данных.

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

Подробнее

www.kaspersky.ru/business