

KASPERSKY SECURITY ДЛЯ БИЗНЕСА

Шифрование данных

Сегодня проактивная защита данных и соответствие отраслевым стандартам безопасности являются общепринятыми требованиями. Технология шифрования «Лаборатории Касперского» предотвращает несанкционированный доступ к данным в случае утери или кражи устройства, на котором они хранятся, или в результате заражения вредоносным ПО, предназначенным для кражи информации.

Благодаря тесной интеграции шифрования с передовыми технологиями защиты рабочих мест наша платформа безопасности позволяет обеспечить защиту данных при их хранении и передаче. Технология шифрования легко развертывается и управляется через централизованную консоль администрирования с использованием единой политики.

Преимущества решения

СООТВЕТСТВИЕ ОТРАСЛЕВЫМ СТАНДАРТАМ

«Лаборатория Касперского» использует признанный в отрасли алгоритм шифрования AES (Advanced Encryption Standard). Поддерживается технология Intel® AES-NI и платформы UEFI и GPT.

ГИБКИЙ ВЫБОР ВИДА ШИФРОВАНИЯ

Для защиты данных на жестких дисках и съемных носителях «Лаборатория Касперского» предлагает различные виды шифрования: шифрование файлов и папок (FLE) и полное шифрование диска (FDE). Специальный портативный режим позволяет использовать и передавать зашифрованные данные на съемных носителях, в том числе на те компьютеры, где ПО для шифрования данных не установлено. Это обеспечивает безопасный обмен данными вне периметра корпоративной сети.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Консоль управления Kaspersky Security Center упрощает настройку параметров шифрования в рамках тех же политик, которые применяются для контроля рабочих мест, безопасности мобильных устройств и других защитных технологий «Лаборатории Касперского».



Технология шифрования «Лаборатории Касперского» обеспечивает беспрепятственный безопасный обмен файлами между пользователями внутри и за пределами периметра корпоративной сети.

Возможности шифрования

ИНТЕГРАЦИЯ С ДРУГИМИ ЗАЩИТНЫМИ ТЕХНОЛОГИЯМИ

Тесная интеграция шифрования с другими защитными технологиями «Лаборатории Касперского», в том числе с инструментами контроля, системного администрирования, а также средствами централизованного управления позволяет построить эффективную многоуровневую систему ИТ-безопасности. Развертывать несколько различных решений и затем управлять ими по отдельности не нужно. Совместимость сетевого оборудования перед развертыванием шифрования проверяется автоматически.

РАЗГРАНИЧЕНИЕ ПРАВ АДМИНИСТРАТОРОВ НА ОСНОВЕ РОЛЕЙ

В крупных организациях со сложной ИТ-инфраструктурой и большим штатом ИТ-специалистов рекомендуется использовать реализованную в решении возможность разделения прав администраторов на основе ролей. Это позволяет упростить процесс управления шифрованием.

ОДНОКРАТНАЯ АВТОРИЗАЦИЯ

Технология шифрования «Лаборатории Касперского» работает с приложениями незаметно для сотрудников, никак не влияя на их производительность. Пользователю достаточно включить компьютер и ввести свои логин и пароль, чтобы получить доступ к Windows и одновременно с этим – ко всем зашифрованным данным на жестком диске компьютера. Авторизация производится до загрузки операционной системы, что обеспечивает дополнительный уровень защиты.

ПОДДЕРЖКА СМАРТ-КАРТ И ТОКЕНОВ

Решение поддерживает двухфакторную аутентификацию посредством смарт-карт и токенов, что устраняет необходимость использования дополнительных логинов и паролей и упрощает работу пользователя.

ВОССТАНОВЛЕНИЕ ДАННЫХ

В решении предусмотрен функционал, позволяющий администратору расшифровать данные в случае аппаратного или программного сбоя. Пользователь может восстановить пароль, вводимый перед загрузкой системы, или получить доступ к зашифрованным данным с помощью механизма секретных вопросов.

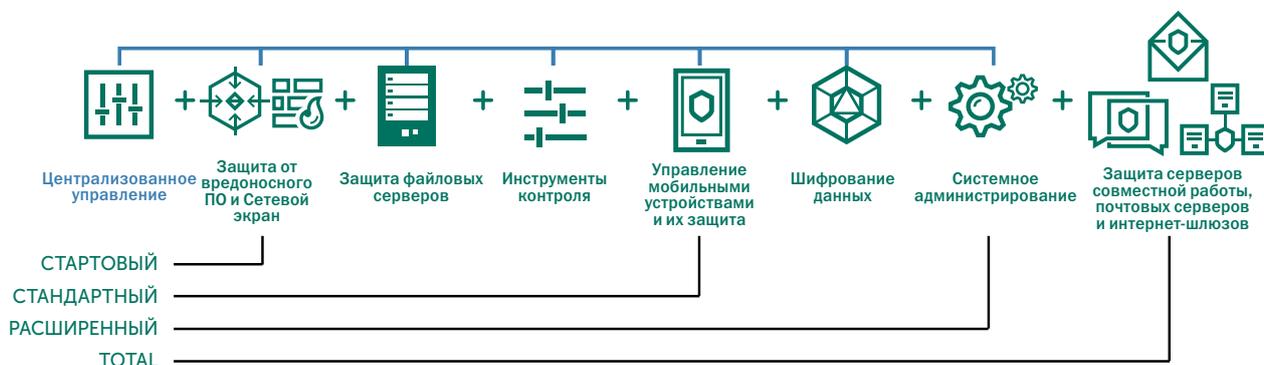
ГИБКИЕ НАСТРОЙКИ РАЗВЕРТЫВАНИЯ

Активация функции шифрования в рамках решений Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ и Kaspersky Total Security для бизнеса не требует установки дополнительного ПО. Вы можете использовать предустановленные параметры шифрования, а также при необходимости изменять их для часто используемых папок, таких как «Мои документы» и «Рабочий стол», новых папок, расширений и групп файлов (например, для документов Microsoft® Office, архивов сообщений электронной почты и т.д.

ВАЖНАЯ ЧАСТЬ ОБЩЕЙ СТРАТЕГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Шифрование данных доступно в составе решений Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ и Kaspersky Total Security для бизнеса. Чтобы приобрести одно из этих решений «Лаборатории Касперского» и надежно защитить ценные данные, обратитесь к нашим партнерам:

http://www.kaspersky.ru/find_partner_office



ПОДРОБНЕЕ:

<http://www.kaspersky.ru/business>