Kingston TECHNOLOGY

Оптимальная безопасность конечных точек объяснение и исследование в партнерстве с Matrix42

MATRIX42

#KingstonIsWithYou

Оптимальная безопасность конечных точек объяснение и исследование в партнерстве с Matrix42

Введение

Защита информации является базовым требованием, предъявляемым к предприятиям, правительствам и отдельным лицам в современном мире.

Утечка данных, взлом и человеческий фактор являются постоянным напоминанием об угрозах и рисках, возникающих во всем мире. Как денежные, так и репутационные издержки, связанные с утечкой данных, могут быть колоссальными. Требования передовых стратегий кибербезопасности и DLP (защиты от потери данных) конечных точек зависят от надежных и эффективных хранилищ данных и памяти.

Использование быстродействующих устройств хранения данных и модулей памяти с функцией шифрования данных в сочетании с лучшими практиками, стандартами и политиками — это большой шаг вперед. Потерянные ноутбуки и USB-накопители подвергают людей и компании риску раскрытия персональной информации. Kingston предлагает решения, которые помогают предотвратить угрозы и снизить риски, в дополнение к существующему или разрабатываемому плану обеспечения безопасности.

Оптимальная безопасность конечных точек объяснение и исследование в партнерстве с Matrix42

Содержание

В этой небольшой электронной книге рассматриваются решения для оконечных устройств, а также то, как USB-накопители Kingston с шифрованием, программа их адаптации и программное обеспечение Matrix42 EgoSecure Data Protection помогли решить задачи в шести различных отраслях и предоставить решение, соответствующее бизнес-потребностям.

Мы подробно рассмотрим эти шесть секторов и как в них решаются проблемы безопасности оконечных устройств.

Содержание

Раздел 1: Пример отрасли государственный сектор

Ситуация:

В государственном секторе очень распространено использование USB-устройств. Например, службы общественного порядка должны копировать фотографии нарушителей правил парковки и административных правонарушений с цифровых камер в системы органов власти через USB-кабель. Правоохранительные органы получают данные расследования на внешних устройствах хранения данных. Эти данные необходимо перезаписать и предотвратить несанкционированный доступ.

Задача:

В связи с высокой потребностью в USB-устройствах сотрудники регулярно запрашивают USB-накопители. Использование личных и неавторизованных устройств хранения данных должно быть заблокировано по соображениям безопасности. Если сотруднику требуется новый USB-накопитель, его следует как можно быстрее предоставить через службу поддержки пользователей, чтобы сотрудники не отвлекались от работы. Важно отметить, что при использовании соответствующих USB-устройств не возникает проблем с безопасностью.

Решение:

Объединив управление устройствами, фильтрацию данных и шифрование, можно реализовать следующий сценарий.

Неизвестные устройства обычно блокируются на оконечных компьютерах. Устройства хранения данных, такие как цифровые камеры, разрешены только для определенных функций, например для чтения файлов изображений. Операции записи обычно шифруются и разрешены только на авторизованных USB-устройствах. Все обращения к данным регистрируются. Управление авторизованными устройствами можно упростить, настроив серийные номера и идентификаторы оборудования. Таким образом, ПО Matrix42 Service Management позволяет пользователю запросить персонализированный USB-накопитель Kingston Technology на портале Self-Service Portal. После процесса утверждения USB-устройство автоматически допускается к использованию в EgoSecure Data Protection.

> “Наши сотрудники рады тому, что новые USB-устройства предоставляются легко и быстро после непродолжительного процесса утверждения. Мы очень довольны программой адаптации Kingston Technology и легкостью администрирования сочетания функций управления услугами и безопасности оконечных устройств в Matrix42.”
>
> **Руководитель службы поддержки, государственный сектор**

Раздел 2: Пример отрасли здравоохранение

Ситуация:

Внешние устройства хранения по-прежнему часто используются как средство обмена данными с сотрудниками и другими организациями.

Например, больницы в Германии должны предоставлять в систему регистрации онкологических больных информацию о текущих случаях заболевания раком и их развитии. Для удобства эти данные часто передаются через мобильные устройства хранения данных.

Врачам также нравится приносить документы, например данные исследований, на свои лекции на USB-накопителях.

Задача:

Данные о пациентах имеют чрезвычайно конфиденциальный характер и не должны попасть в руки посторонних лиц. Следовательно, необходимо усилить защиту данных. Утеря носителя данных может стать серьезной проблемой не только из-за требований GDPR, но и благополучия пациентов. Поэтому очень важен контроль, отслеживание и шифрование доступа к USB-накопителю.

Решение:

EgoSecure Data Protection объединяет различные меры защиты, такие как контроль доступа, аудит данных, фильтрация и шифрование, в одном решении. ИТ-администраторы могут решать, каким сотрудникам и к каким устройствам будет предоставлен доступ. Возможны исключения, например, по серийному номеру и идентификатору оборудования. Эти идентификаторы могут быть определены с помощью программы адаптации Kingston Technology, так что в системе управления EgoSecure Data Protection потребуется настроить только одно значение, чтобы разрешить использование только устройств, одобренных компанией. Это значительно сокращает усилия по администрированию и повышает безопасность данных (согласно GDPR, CCPA, HIPAA и т. д.), поскольку доступ к данным зашифрован и отслеживается.

> “Мы уже использовали USB-накопители Kingston с шифрованием. Теперь, с помощью EgoSecure Data Protection, мы также можем гарантировать, что отслеживаемость передачи данных пациентов осуществляется в соответствии с требованиями GDPR ЕС.”
>
> **директор по информационной безопасности, университетская клиническая больница**

Раздел 3: Пример отрасли финансы

Ситуация:

К банкам предъявляются различные нормативные требования. Одним их них являеся PCI-DSS (стандарт защиты информации в индустрии платежных карт). Требования PCI-DSS включают необходимость шифрования данных, анализа уязвимостей и фильтрации данных. Цель состоит в том, чтобы минимизировать или полностью предотвратить угрозы и риски ИТ-безопасности.

Задача:

С оконечными устройствами связано множество рисков с точки зрения безопасности ИТ. Сотрудники должны работать с информацией о платежных картах от потребителей и предприятий и ежедневно обрабатывать конфиденциальные данные финансовых учреждений. В результате возникает риск того, что данные из облака, электронной почты, USB-накопителей и Интернета могут быть скомпрометированы вредоносным ПО или могут случайно попасть в руки третьих лиц, если не будут должным образом защищены. Подобный инцидент имел бы финансовые последствия для банка с точки зрения GDPR, PCI-DSS, а также закона Сарбейнса-Оксли. Кроме того, киберпреступники пытаются различными способами влиять на банковские системы или манипулировать ими, и становятся в этом все более и более изобретательными. Совсем недавно, например, было совершено киберпреступление, связанное с банкоматами: в них было отключено питание, и система была запущена с загрузочного USB-устройства с целью кражи денег.

Решение:

ИТ-системы должны быть защищены с помощью многоуровневых мер безопасности. Для этого можно использовать управление приложениями и устройствами, обнаружение аномалий, UEBA (анализ поведения пользователей и объектов), мониторинг и полное шифрование диска с помощью PreBoot Authentication. Matrix42 позволяет внедрить все эти меры в автоматизированной и целостной экосистеме, допускающей использование только разрешенных приложений и USB-устройств с шифрованием. Кроме того, если обнаруживается подозрительная или вредоносная активность, меры принимаются автоматически. Что касается использования USB-накопителей, сочетание адаптируемых USB-накопителей от Kingston Technology помогает обеспечить включение устройств в белый список с минимальными усилиями, а также надежное и отслеживаемое шифрование данных. Это существенно улучшает соответствие нормативным требованиям и не требует дополнительных трудозатрат.

> “Используя EgoSecure Data Protection и функциональность белого списка, мы допускаем одобрение только USB-накопителей Kingston с шифрованием. Мы заносим в белый список USB-накопители Kingston с шифрованием с персональным идентификатором оборудования — использование других устройств запрещено. Это существенно сокращает трудозатраты на администрирование и в то же время повышает безопасность!”

ИТ-менеджер, финансовая компания

Раздел 4: Пример отрасли автомобилестроение

Ситуация:

В отрасли автомобилестроения USB-накопители используются в разных областях. Например, данные исследований хранятся на внешних накопителях для обмена между соответствующими инженерами компании. Для настройки производственных машин файлы переносятся из ИТ-среды в рабочую среду. Все эти данные являются строго конфиденциальными и должны быть защищены от промышленного шпионажа и кражи, иначе накопленные научно-технические наработки могут попасть в чужие руки.

Задача:

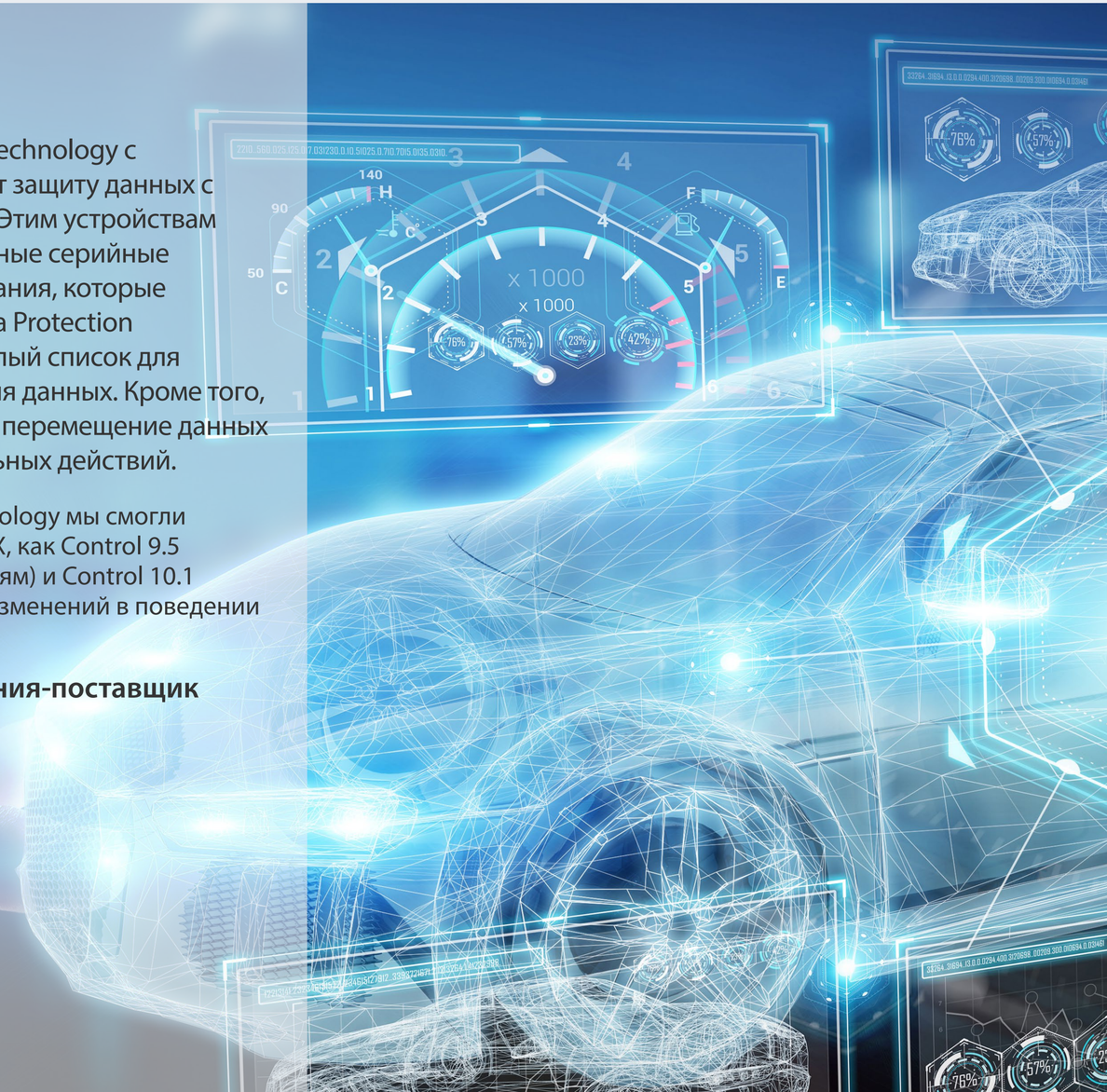
Автомобильная промышленность подчиняется нормативным требованиям, таким как TISAX, защита прототипов, ENX, ISO27001, «стороннее подключение» и GDPR. Статьи Control 9.1, 9.5 и 10.1 стандарта TISAX требуют, чтобы обращения к данным контролировались, отслеживались, фильтровались и шифровались. Эти меры должны соблюдаться и в отношении других нормативных требований, таких как GDPR и ISO27001, во всех сферах деятельности автомобилестроительных компаний.

Решение:

USB-накопители компании Kingston Technology с функцией шифрования обеспечивают защиту данных с помощью аппаратного шифрования. Этим устройствам можно назначить персонализированные серийные номера и идентификаторы оборудования, которые можно использовать в EgoSecure Data Protection для автоматического включения в белый список для конкретных сценариев использования данных. Кроме того, можно отслеживать и анализировать перемещение данных при наличии каких-либо подозрительных действий.

> “Благодаря Matrix42 и Kingston Technology мы смогли реализовать такие требования TISAX, как Control 9.5 (доступ к информации и приложениям) и Control 10.1 (криптография), без значительных изменений в поведении пользователей.”

технический директор, компания-поставщик автомобильных компонентов



Раздел 5: Пример отрасли телекоммуникации

Ситуация:

Провайдеры телекоммуникационных услуг получают много информации о клиентах. Эта информация является строго конфиденциальной, особенно с точки зрения регламента GDPR. Следовательно, необходимо принимать действенные меры для предотвращения потери и кражи данных.

Задача:

Сотрудники телекоммуникационных компаний ежедневно работают с данными клиентов. Большая часть этих данных хранится в бизнес-приложениях. Однако существует риск того, что контракты с клиентами или даже данные, экспортированные из базы данных, будут храниться на оконечном устройстве и подключенных к нему внешних устройствах. Для обмена данными пользователи часто используют внешние устройства хранения. Поэтому очень важно выявлять и устранять ненадлежащие практики хранения данных и обеспечивать соответствующую защиту.

Решение:

Чтобы упростить процесс закупки, USB-накопители с шифрованием от Kingston Technology с персонализированным идентификатором продукта можно быстро приобрести через предварительно определенный белый список в EgoSecure Data Protection и получить через каталог услуг Matrix42. Хранение и экспорт данных, которые могут содержать конфиденциальную информацию, могут автоматически идентифицироваться и корректироваться с помощью глубокого анализа контента на основе сканирования «используемых данных» и «хранящихся данных». Перемещение данных регистрируется централизованно. Таким образом, сотрудник может быстро получить новое оборудование для хранения данных после его запроса и одобрения. Это позволяет гарантировать соблюдение требований GDPR.

> “Благодаря порталу самообслуживания Matrix42 наши пользователи могут быстро запрашивать устройства хранения, когда в них возникает необходимость. После одобрения заказа и доставки устройства оно допускается к использованию контролем устройств EgoSecure. Сочетание предложений Matrix42 и Kingston Technology повышает производительность и безопасность в нашей компании.”

Технический директор, поставщик телекоммуникационных услуг

Раздел 6: Пример отрасли
Промышленное производство

Ситуация:

Валюта будущего — это цифровые данные. Эти ценные данные в различных отраслях промышленности включают планы производства, данные о клиентах и поставщиках, а также научно-технические наработки компании. Утеря этих данных может привести не только к очень серьезным штрафам в соответствии с GDPR, но также к быстро растущим и репутационным проблемам. К сожалению, множество USB-накопители каждый день теряют в такси, прачечных, в аэропортах, на вокзалах или на парковках.

Задача:

Устройства хранения часто содержат строго конфиденциальные данные, и, к сожалению, эти данные часто не зашифрованы. Также существует риск того, что технические специалисты по обслуживанию используют внешние носители данных для установки обновлений для производственных машин. Эти внешние устройства несут риск занесения вредоносных программ в сеть.

Решение:

USB-накопители компании Kingston Technology с функцией шифрования обеспечивают защиту данных с помощью аппаратного шифрования. Эти устройства могут поставляться с персонализированными серийными номерами и идентификаторами оборудования, которые можно использовать в EgoSecure Data Protection для автоматического включения в белый список для конкретных сценариев использования данных. Кроме того, можно отслеживать и анализировать перемещение данных при наличии каких-либо подозрительных действий.

> “Шифрование наших производственных данных имеет очень важное значение для защиты от кражи данных. Эти строго конфиденциальные данные допускается хранить только на одобренных Kingston USB-накопителях с шифрованием посредством фильтрации файлов с помощью EgoSecure Data Protection. На всех других USB-устройствах производственные данные блокируются, а доступ для записи на внешние устройства хранения данных защищается оперативным шифрованием и журналированием EgoSecure.”
>
> **Ответственный за безопасность ИТ, промышленное производство**

Раздел 7: Решения Kingston и Matrix42

Использование шифрования, быстрого хранилища и памяти в сочетании с передовыми практиками, стандартами и политиками - большой шаг. Потерянные ноутбуки и USB-накопители подвергают людей и компании риску раскрытия персональной информации. Kingston Technology предлагает решения, которые помогают предотвратить угрозы и снизить риски, в дополнение к существующему или разрабатываемому плану обеспечения безопасности.

USB-накопители с шифрованием от Kingston Technology

USB-накопители с аппаратным шифрованием от Kingston Technology оснащены функциями защиты данных с внутренней и внешней стороны брандмауэра организации. Разработанные в целях защиты информации, для которой требуется обеспечение сверхнадежной безопасности, эти накопители помогут вам соблюдать конкретные промышленные стандарты, директивы и правила. Продукты соответствуют требованиям TAA, сертифицированы FIPS и доступны в вариантах емкости до 128 ГБ. Они идеально подходят как для корпоративных пользователей, так и для государственных учреждений.

Программа безопасной настройки

Вы можете настраивать USB-накопители с шифрованием от Kingston Technology в соответствии с потребностями вашей компании. Добавьте выбранные функции для создания уникальных накопителей. Kingston Technology предоставляет возможность быстрого и удобного заказа настраиваемых USB-накопителей с шифрованием через вашего реселлера. Линейка USB-продукции Kingston Technology с шифрованием включает серии DTVP30, DT4000G2 и IKD300S. Эта программа предоставляет дополнительные возможности для настройки, наиболее востребованные заказчикам, в том числе серийные номера, двойные пароли и пользовательские логотипы. В рамках программы можно заказать минимум 50 единиц продукции (с повторным заказом 25 единиц) в точном соответствии с потребностями организации.

ПО EgoSecure Data Protection от Matrix42

ПО EgoSecure Data Protection от Matrix42 предоставляет компаниям возможность комплексного управления безопасностью для предотвращения нарушений и защиты устройств, систем и данных. Решение автоматизирует весь процесс, начиная от предотвращения и обнаружения нарушений до принятия мер в случае ущерба без потери производительности.

Выводы

Обеспечение защиты данных и кибербезопасности могут казаться сложной задачей. Требования к работе с цифровыми устройствами значительно изменились: сотрудники получили возможность самостоятельно решать, когда, где и с какими устройствами им работать. Правильное сочетание USB-накопителей с аппаратным шифрованием и программным управлением оконечными устройствами может помочь организациям обеспечить контроль над своими устройствами. Таким образом, снижается риск утечки данных и поддерживается текущая стратегия соблюдения требований GDPR.

О компании Kingston

Основываясь на более чем 30-летнем опыте работы, Kingston Technology обладает знаниями для выявления и решения проблем безопасности оконечных устройств без ущерба для вашей организации.

#KingstonIsWithYou