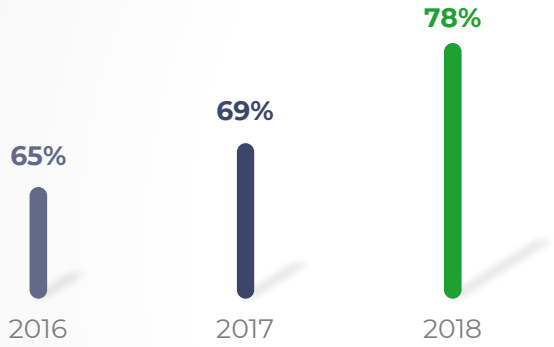
EVERYTAG

Необходимый элемент информационной безопасности

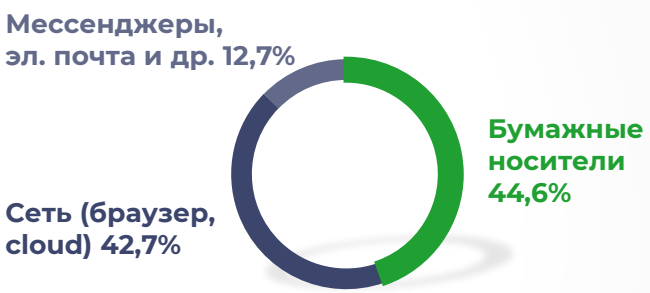
Защита важной информации и предотвращение утечек

78% УТЕЧЕК ИНФОРМАЦИИ В РОССИЙСКИХ КОМПАНИЯХ ПРОИСХОДИТ ПО ВИНЕ СОТРУДНИКОВ, А НЕ ИЗ-ЗА ВНЕШНИХ ЗЛОУМЫШЛЕННИКОВ

Процент утечек по вине сотрудников



Распределение утечек информации по каналам



Сотрудники делают скриншоты информационных систем с коммерческой информацией, пересылают файлы ограниченного доступа по электронной почте, фотографируют документы на телефон и распечатывают конфиденциальные данные на бумаге.

ПОЧЕМУ КОМПАНИИ СТРЕМЯТСЯ ЗАЩИТИТЬ ИНФОРМАЦИЮ?

УЯЗВИМОСТЬ ИНФОРМАЦИИ, ОТОБРАЖАЕМОЙ В ВЕБ-ИНТЕРФЕЙСАХ

Любой сотрудник, у которого есть доступ к персональным данным клиентов, может просто сфотографировать экран. Это касается и биллинговых систем, и данных внутри CRM, и отдельно взятых документов.

УЯЗВИМОСТЬ ИНФОРМАЦИИ НА БУМАЖНЫХ НОСИТЕЛЯХ

Распечатанную информацию, например, внутренние отчёты, неподлежащие разглашению договоренности или даже результаты исследований и разработок, можно сфотографировать или просто передать третьим лицам.

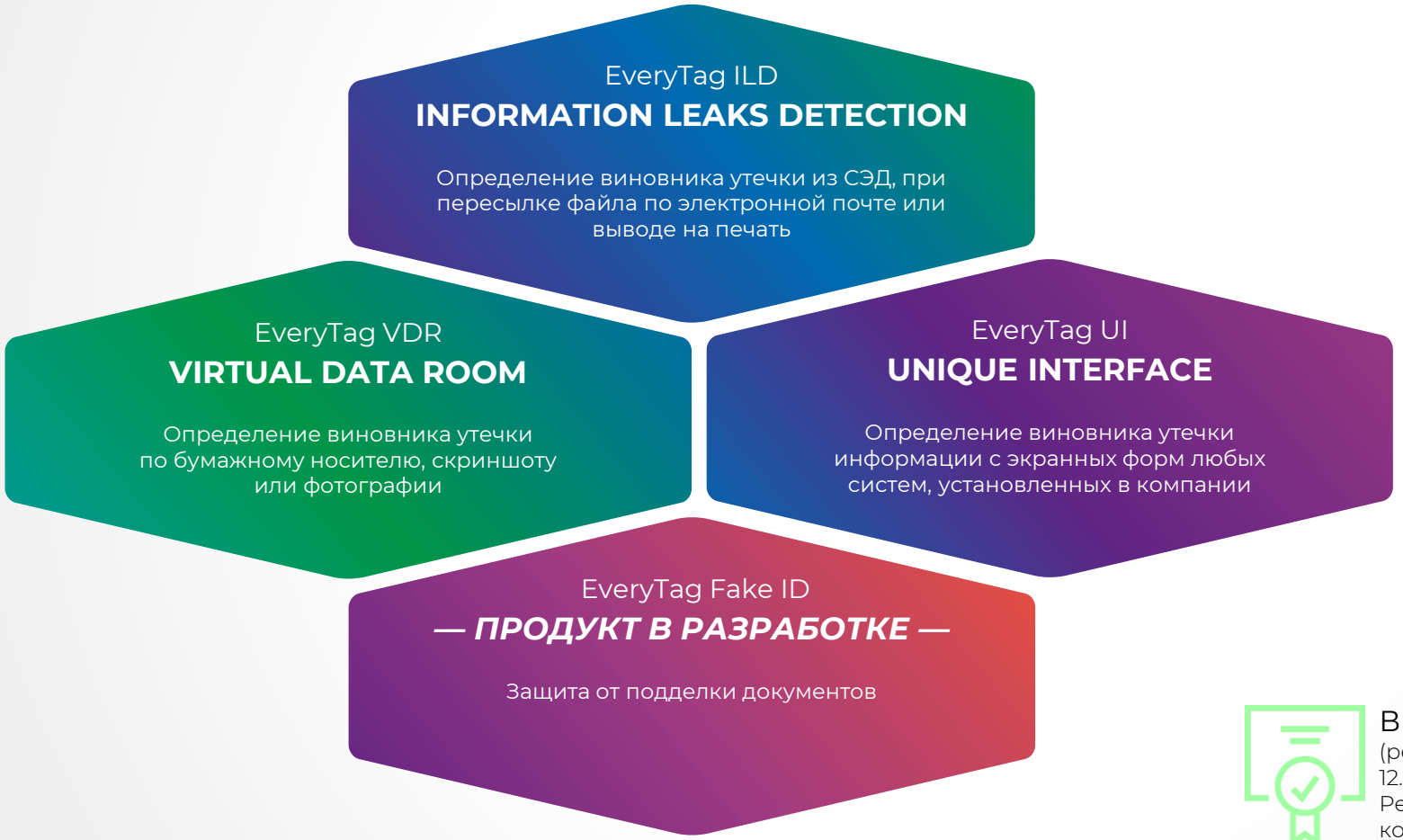
УЯЗВИМОСТЬ ПРОЦЕССА ОБМЕНА ИНФОРМАЦИЕЙ С КОНТРАГЕНТАМИ

Например, в рамках аудиторских проверок или проведения финансово-юридической экспертизы компаниям необходимо предоставлять доступ к важным документам сотрудникам внешних контрагентов.

НЕОБХОДИМА ТАКАЯ СИСТЕМА ЗАЩИТЫ ОТ УТЕЧЕК, КОТОРАЯ:

- исключит анонимность и безнаказанность
- безошибочно установит виновника утечки
- прозрачно встроится в существующие бизнес-процессы
- идентифицирует, кем распечатан или сфотографирован документ
- работает со всеми форматами файлов, содержащими чувствительную информацию
- является кросс-платформенной и не требует сложного обслуживания

РЕШЕНИЯ EVERYTAG ЗАЩИЩАЮТ КОМПАНИИ ОТ УТЕЧЕК ИНФОРМАЦИИ



Внесены в реестр ПО Минкомсвязи РФ
(рег. номер ПО 4464, Приказ Минкомсвязи России от 12.04.2018 №157)
Рекомендованы к использованию российскими компаниями и госучреждениями.

EveryTag ILD

INFORMATION LEAKS DETECTION

Прозрачное встраивание в критически важные источники данных (ECM, почта, печать) без изменения привычных бизнес-процессов

EveryTag ILD — ЭТО ПРОЗРАЧНАЯ ЗАЩИТА ДОКУМЕНТОВ ОТ УТЕЧКИ

Обменивайтесь документами через существующую СЭД или по электронной почте, а также отправляйте их на печать — документы в любом случае будут защищены алгоритмом EveryTag ILD.

КАК ЭТО РАБОТАЕТ:

EveryTag ILD интегрируется в действующую систему электронного документооборота, и оставаясь незаметным для пользователей.

При каждом открытии или отправке документ незаметно маркируется, и конечный пользователь получает уникальную копию, визуально не отличимую от оригинала.

Алгоритм EveryTag ILD безошибочно определит виновника утечки по уникальной невидимой маркировке документа.

Кейсы использования EveryTag ILD

Определить виновника раскрытия коммерческой тайны

Раскрытие коммерческой тайны может подорвать отношения с партнерами и привести к убыткам.

Сценарий:

У сотрудников компании есть доступ к коммерческой информации, которая требуется им для работы.

Один из сотрудников передает информацию, предназначенную для партнёра А, в руки представителя партнёра Б.

Отношения с партнёром Б ухудшаются (уход к конкурентам, пересмотр условий сотрудничества и тд), компания теряет часть выручки.

Компания проводит расследование и идентифицирует сотрудника, раскрывшего коммерческую тайну.

Идентифицировать сотрудника, допустившего утечку внутренних документов

Воровство внутренних разработок, официальных писем, результатов экспертиз и других чувствительных документов может привести к репутационным и финансовым потерям.

Сценарий:

Компания разрабатывает новый продукт.

Сотрудник фотографирует данные с планами компании и продает их в СМИ.

СМИ публикуют резонансную информацию.

Продажи текущего продукта падают, компания несёт убытки.

Компания проводит экспертизу и выясняет, кто допустил утечку информации до официального релиза нового продукта.

Техническая информация о системе EveryTag ILD

РОЛИ ВНУТРИ СИСТЕМЫ

Пользователь

Секретарь

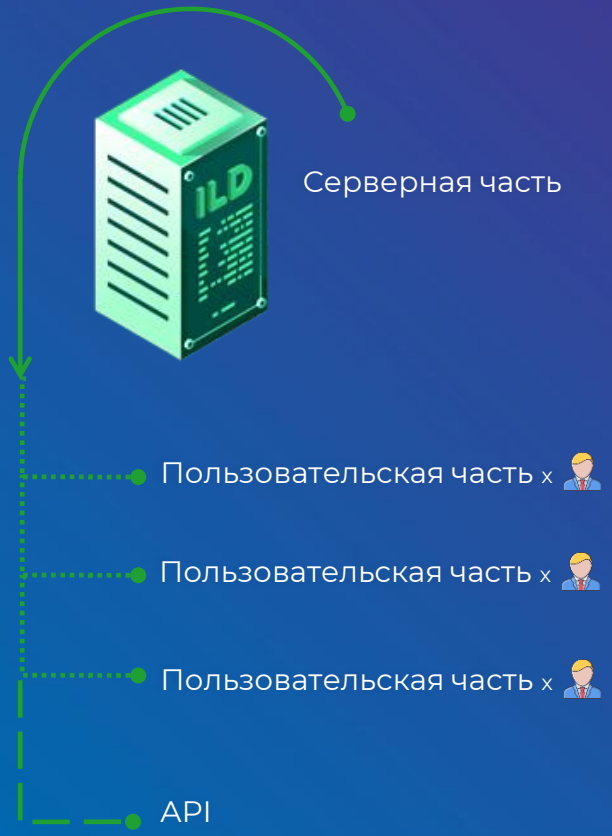
Специалист по безопасности

ВАРИАНТЫ РАЗВЁРТЫВАНИЯ:

на собственном сервере

на облачном сервере

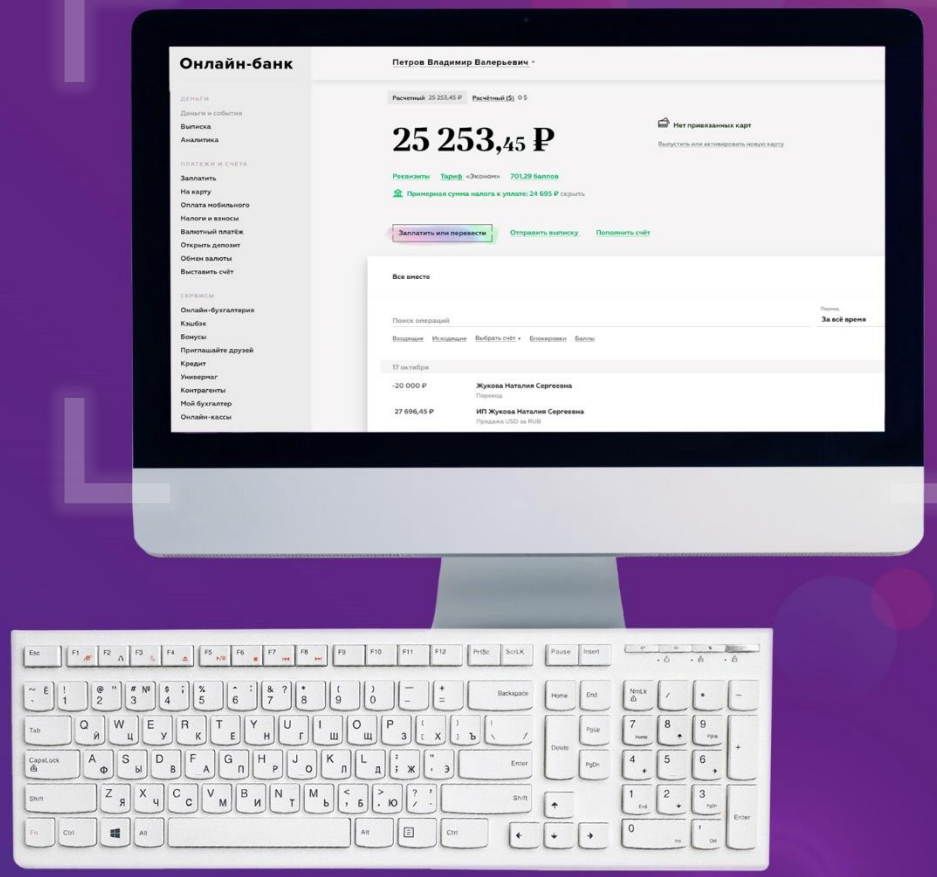
ВАРИАНТЫ ПОСТАВКИ



EveryTag UI

UNIQUE INTERFACE

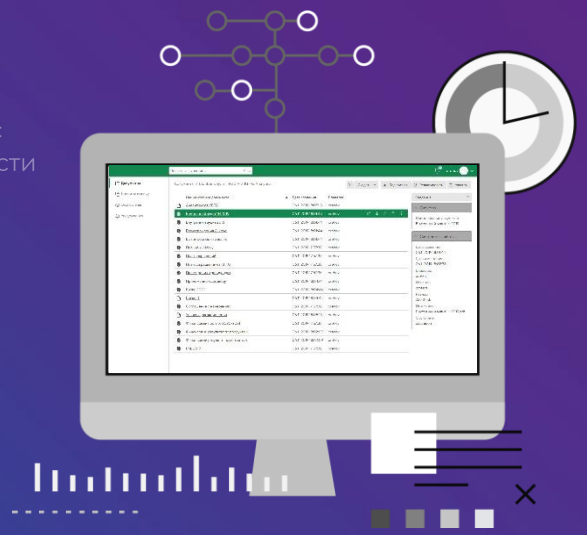
Защита от утечек чувствительной информации
через экранные формы и скриншоты



EveryTag UI — ЭТО ЗАЩИТА ОТ УТЕЧКИ ИНФОРМАЦИИ С ЭКРАННЫХ ФОРМ

Установите EveryTag UI на клиентском сервере, и он прозрачно встроится в существующие информационные системы вашей компании.

EveryTag UI имеет удобный веб-интерфейс для офицера безопасности



КАК ЭТО РАБОТАЕТ:

EveryTag UI незаметно маркирует интерфейс информационной системы пользователя. Таким образом, экранная форма каждого пользователя уникальна.

Если пользователь допустит утечку скриншота системы с чувствительной информацией, алгоритм EveryTag UI позволит оперативно установить нарушителя.

Кейс использования EveryTag UI: Телеком-компания

СОТРУДНИК ПРОДАЕТ ИНФОРМАЦИЮ ИЗ БИЛЛИНГОВОЙ СИСТЕМЫ В ДАРКНЕТЕ

Многие компании работают с данными клиентов внутри сторонник систем, например, CRM или ERP. Доступ к системам необходим сотрудникам колл-центра для работы. Продажа информации о пользователях — уже привычная «подработка» для таких сотрудников. По запросу они фотографируют экран с данными из биллинговой системы и получают за это вознаграждение.

Проблема:

СМИ и/или клиенты компании узнают, что персональные данные клиентов можно за небольшую сумму получить через специализированные каналы «пробивки» данных на черном рынке.

Решение

Компания проводит серию расследований с образцами информации, определяет сотрудников, продающих данные и предпринимает меры.

EveryTag VDR

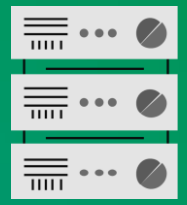
VIRTUAL DATA ROOM

Контролируемая, защищённая от утечек работа
всех пользователей с электронными документами
и их бумажными копиями

EveryTag VDR — ЭТО БЕЗОПАСНОЕ ПРОСТРАНСТВО ОБМЕНА ДОКУМЕНТАМИ

Загружайте документы, обменивайтесь ими с другими пользователями и будьте уверены в безопасности.

ВАРИАНТЫ РАЗВЁРТЫВАНИЯ:



на собственном сервере

на облачном сервере

КАК ЭТО РАБОТАЕТ:

Каждый раз VDR отображает пользователю вместо оригинального файла его уникальную маркированную копию, которая визуально неотличима от оригинала. При этом в системе сохраняется информация о том, кто открыл документ, когда и на каком устройстве.

Вы защищены от утечки, так как при её возникновении вы сможете безошибочно определить, кто из пользователей эту утечку допустил.

Алгоритм защиты EveryTag VDR может идентифицировать виновника утечки по скриншоту, целому бумажному документу или его фрагменту, а также по фотографии печатного документа.

Кейсы использования EveryTag VDR

Утечка в результате халатности сотрудников и нарушения ими внутренних правил

Конфиденциальная информация, может быть доступна для присвоения и копирования сторонними лицами в результате халатности сотрудников и нарушения ими внутренних правил.

Сценарий:

Конфиденциальный документ был распечатан для совещания.

Сотрудник оставил документ в переговорной комнате.

После совещания в помещении была встреча с клиентом.

Клиент после встречи использовал документ как рычаг в переговорах.

Компания провела экспертизу и выяснила, чьи действия привели к инциденту.

Утечка в результате умышленных действий пользователей

Важная информация может попасть в руки третьих лиц или СМИ в результате умышленных действий пользователей.

Сценарий:

Условия соглашения между компаниями обсуждаются юристами и другими вовлеченными в процесс людьми.

Кто-то из участников процесса фотографирует экран с информацией, которая содержится в соглашении, и передает её в медиа.

СМИ публикуют громкий анонс с подтверждением в виде фотографии документа.

Сделка срывается, акции падают.

Компании проводят экспертизу и выясняют, кто допустил утечку информации до официального объявления.

EveryTag FakeID

— ПРОДУКТ В РАЗРАБОТКЕ —

Система защиты документов от подделки

СИСТЕМА ПРОВЕРКИ ПОДЛИННОСТИ ДОКУМЕНТОВ

Заверяйте важные документы с помощью нового решения EveryTag и сохраняйте их в локальной системе компании. Все получатели системы смогут в дальнейшем проверить подлинность копии документа или его фрагмента.

Решение EveryTag работает с любыми документами, содержащими текст: офисные пакеты (текстовые и табличные процессоры, презентации), чертежи, графики, pdf-файлы, а также сканированные копии или фотографии документов.

КАК ЭТО РАБОТАЕТ:

Подписывая документ с помощью нового решения EveryTag, пользователь наделяет его уникальным цифровым почерком. Впоследствии все получатели могут проверять этот документ на подлинность и целостность (отсутствие изменений).

скоро!

EVERYTAG

**Защищаем там,
где другие бессильны**

+7 (495) 008 16 95

partners@everytag.ru