

BRILLIX

Поиск и маскирование конфиденциальных данных

- ✗ Маскирование реальных данных
- ✗ Защита конфиденциальных данных
- ✗ Предотвращение утечки данных
- ✗ Сохранение конфиденциальности
- ✗ Обнаружение схем данных
(для производственных и непроизводственных сред)
- ✗ Автоматическое оповещение для предотвращения утечки данных
(тестирование, разработка, обеспечение качества, обучение, интеграция и т.д.)
- ✗ Регулирование и соответствие: Общие правила защиты данных ЕС (GDPR), PCI-DSS

ITD Group
International IT Distribution

ITD Group

Эксклюзивный дистрибутор

<http://www.iitdgroup.ru>

info@iitdgroup.ru

+7(499) 502-1375



О продукте JumbleDB

JumbleDB - простое, надёжное и интуитивно понятное решение для обнаружения, классификации и маскировки данных. Он обеспечивает **быстрый** и **интеллектуальный** механизм автоматического обнаружения данных, основанный на готовых шаблонах, с поддержкой нескольких гетерогенных баз данных.

JumbleDB обеспечивает **реальные** и **значимые** альтернативные данные подменяя конфиденциальные, сохраняя целостность бизнеса, сохраняя ваши данные в их первоначальной структуре, обеспечивая непрерывность работы ваших бизнес-приложений.

JumbleDB - это **комплексное** универсальное решение **для всех ваших задач** обнаружения и маскирования конфиденциальных данных.

Маскирование Реальных Данных

Маскирование данных, также называемое анонимизацией данных и псевдонимизацией*, является методом полного скремблирования** и обфускации*** данных, одновременно уменьшая связывание набора данных с исходным идентификатором субъекта данных. Обычно это делается для того, чтобы уменьшить риск случайного или преднамеренного раскрытия информации, сделав информацию не идентифицируемой с физическим или юридическим лицом.

Маскирование данных — метод создания структурно-подобной, но неаутентичной версии данных организации, которые могут использоваться для таких целей, как тестирование программного обеспечения и обучение пользователей. Цель состоит в том, чтобы защитить фактические данные, имея полнофункциональную замену, в случаях, когда реальные данные не требуются.

Маскирование данных часто используется для скрытия персональных данных и предотвращения разглашения персональных данных в слабо защищённых средах, таких как среды тестирования и разработки. Хотя большинство организаций имеют строгие меры безопасности для защиты конфиденциальных данных при обработке, иногда те же данные



используются для менее защищённых операций. Эта проблема часто усугубляется, если эти операции передаются на аутсорсинг, и организация имеет меньший контроль над данными. Вследствие законодательства о защите конфиденциальной информации большинство организаций перестают раскрывать реальные данные без необходимости.

При маскировке данных формат данных остаётся неизменным; изменяются только значения. Данные могут быть изменены несколькими способами, включая шифрование, перетасовку символов, и замену символов или слов. Какой бы метод Вы ни выбрали, значения должны быть каким-то образом изменены так, чтобы сделало невозможным обратное восстановление данных.

* **Псевдонимизация** – процесс, посредством которого поля в записи данных, позволяющие идентифицировать конкретное лицо, заменяются одним или несколькими искусственными идентификаторами или псевдонимами.

** **Скремблирование** – процесс преобразования набора данных с целью получения свойств случайной последовательности.

*** **Обфускация** – процесс приведения исходных данных к виду, сохраняющему их функциональность, но затрудняющему анализ и понимание.

Конфиденциальные данные	ID	Name	Credit Card
	12345678-9	Kobi Peretz	4580-1111-2222-3333
	98765432-1	Dudu Aharon	5326-1003-1234-2222
	45678932-5	Eyal Golan	4580-9999-4444-5555
Маскирование данных: перестановка	ID	Name	Credit Card
	98765432-1	Kobi Peretz	4580-1111-2222-3333
	45678932-5	Dudu Aharon	5326-1003-4444-55555
	12345678-9	Eyal Golan	4580-9999-6666-7777
Маскирование данных: замена значений	ID	Name	Credit Card
	98765432-1	Kobi Peretz	4580-1111-2233-4455
	45678932-5	Dudu Aharon	5326-1003-4455-6677
	12345678-9	Eyal Golan	4580-9999-6677-8899

Рисунок 1 – Маскирование физических данных: до и после (2 примера)



Инновационный подход к маскировке реальных данных

JumbleDB - простое, надёжное и интуитивно понятное решение для обнаружения и маскирования данных, которое позволяет организациям проводить эффективное и быстрое маскирование конфиденциальных данных. Это уникальное решение позволяет специалистам по информационной безопасности наряду с персоналом, ответственным за базы данных и инфраструктуру, эффективно выполнять скремблирование данных, одновременно соблюдая различные правила и требования, включая **PCI**, **GDPR** и другие.



JumbleDB основывается на уникальном трёхуровневом подходе:

Обнаружение → Защита → Предупреждение

Этот уникальный подход позволяет осуществлять непрерывное скремблирование конфиденциальных данных и постоянное наблюдение за скремблированными данными в производственных средах.

Шаг Первый: Обнаружение

Первым шагом является обнаружение конфиденциальных данных в базе данных. Используя инструмент обнаружения конфиденциальных данных, вы можете:

- Обнаруживать и идентифицировать конфиденциальные данные с помощью интеллектуальных поисковых систем, с обширной предопределённой и расширяемой библиотекой шаблонов важных данных;



- Обнаруживать и определять, где находятся конфиденциальные данные в вашей базе данных, в соответствии с содержанием, структурой данных и именами столбцов;
- Обнаруживать взаимосвязи в базе данных: связи, определяемые в базе данных (внешние ключи), а также связи, определённые различными приложениями.

Шаг Второй: Защита

Второй шаг - маскирование данных и скремблирование:

- Различные алгоритмы скремблирования, которые разработаны и адаптированы для обработки очень больших объёмов данных;
- Обширная и расширяемая библиотека форматов анонимизации и маскировки, функций преобразования данных и различных шаблонов;
- Легко маскирует и скремблирует личные данные и любые другие типы конфиденциальных данных, такие как номера кредитных карт, национальные идентификаторы и другую личную информацию благодаря обширной библиотеке форматов маскировки и скремблирования;
- Добавляйте собственные методы скремблирования и маскировки ваших конфиденциальных данных;
- Алгоритмы маскировки предоставляют значимые данные, сохраняя при этом целостность информации.

Шаг Третий: Предупреждение

Третий шаг - предотвращение утечки конфиденциальных данных:

- Убедитесь, что даже после успешного завершения проекта скремблирования никакие конфиденциальные данные не будут импортированы и введены в незащищённые среды бесконтрольно;
- Предотвращение утечки конфиденциальных данных и автоматическое оповещение о данных и структурных изменениях;
- Пользователи будут автоматически получать уведомления, когда важные данные добавляются в уже замаскированную среду базы данных.



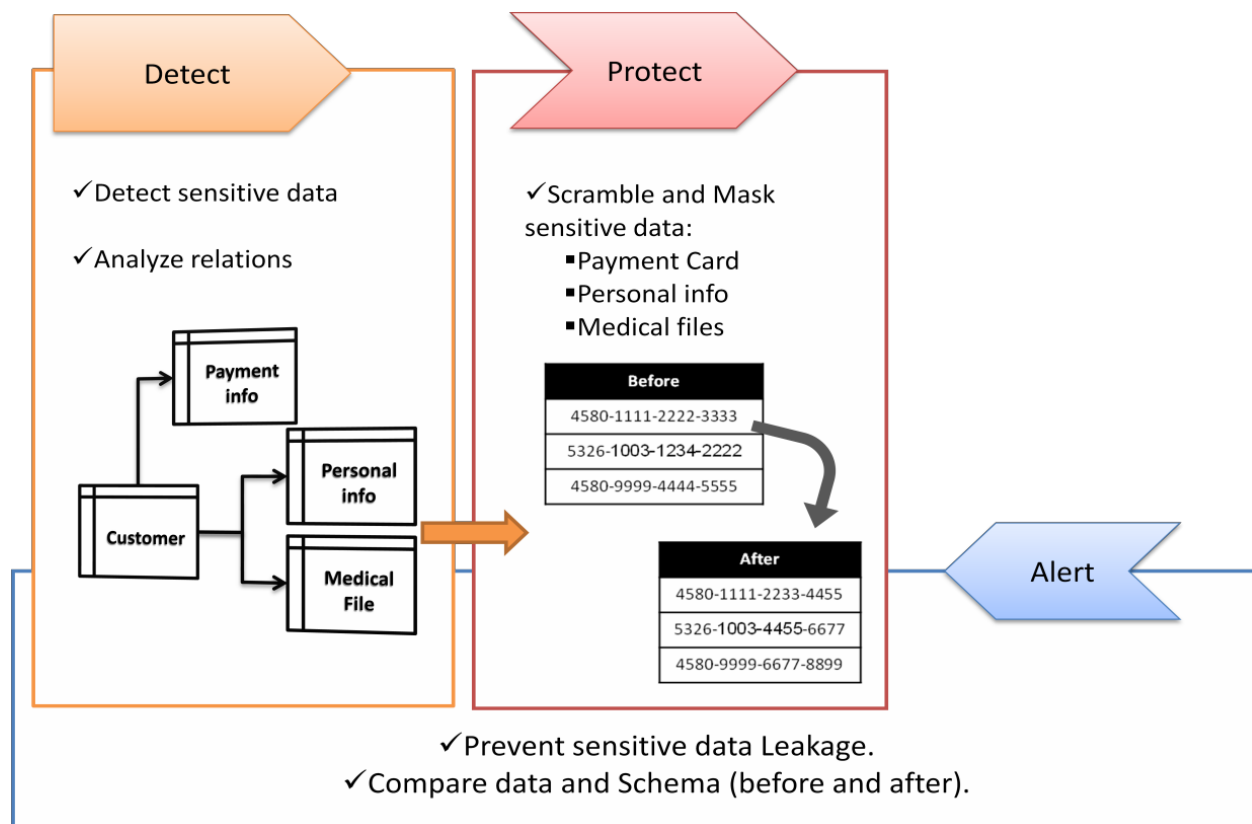


Рисунок 2 – Инновационный подход к проекту маскирования важных данных

Основные функции JumbleDB:

- Насыщенный и сразу готовый к использованию словарь классификации данных;
- Предопределённые и расширяемые алгоритмы маскировки пользовательских конфиденциальных данных;
- Автоматическое обнаружение и анализ взаимосвязей конфиденциальных данных;
- Поддержка общности и целостности информации на основе гетерогенных платформах баз данных;
- Оптимизированные алгоритмы скремблирования для обработки чрезвычайно больших объёмов данных;



- Автоматический механизм оповещения для мониторинга и предотвращения утечки конфиденциальных данных;
- Централизованное решение для обнаружения и скремблирования конфиденциальных данных;
- Простая и быстрая установка и развёртывание;
- Предварительный просмотр маскировки и скремблирования;
- Поддержка большинства распространённых реляционных баз данных: Oracle, Microsoft SQL Server, MySQL, DB2.

О компании Brillix Ltd.

С 2007 года мы стремимся разрабатывать и внедрять лучшие в своём классе инновационные технологии и решения для ваших платформ баз данных, защиты данных и больших сред данных. Мы стремимся обеспечить наивысшее качество продукции и услуг, предоставляемых нашей всемирно признанной командой экспертов.

О компании ITD Group

International IT-Distribution Group (**ITD Group**) – группа компаний, представляющая интересы разработчиков инновационных решений в сфере защиты информации.

Компания была создана в 2007 году и уже более 10 лет активно продвигает на российском рынке и рынке стран СНГ решения, основанные на уникальных IT технологиях, призванные обеспечивать комплексную информационную защиту данных и компьютерных сетей.

ITD Group является официальным дистрибьютором продукции **Brillix Ltd.**

