Data Mask

Универсальное решение по маскированию данных

О компании Secret Technologies

SecretTechnologies

семейство продуктов*

Secret Cloud

безопасный файловый обмен с сотрудниками и партнерами. SCE сертифицирован ФСТЭК РФ по 4 уровню доверия

DataMask

обезличивание чувствительных данных

с 2016 года

на рынке ИБ

Trace Doc

создание уникальных копий документов

VideoAnalyzer

система автоматизированного анализа видео- и аудиоархивов

> 100 тысяч

пользователей продуктов

Screen Guard

защита экрана монитора от фотографирования

Printer Guard

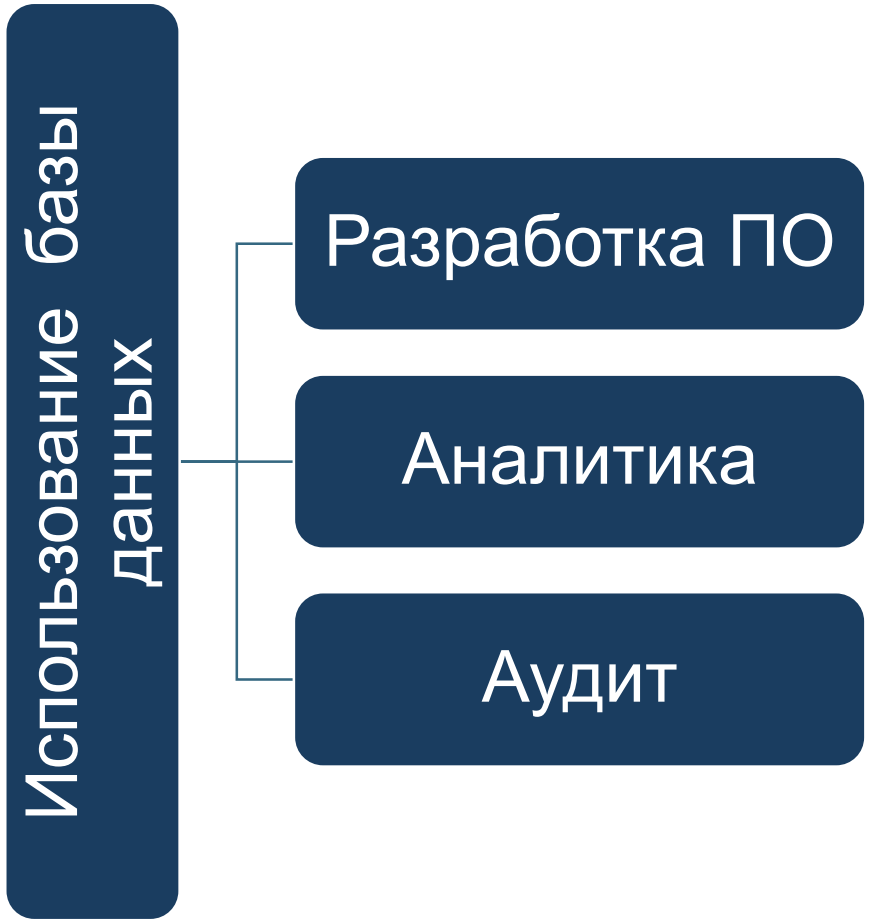
контроль и экономия печати

8 продуктов

в собственном портфеле решений

*В семейство продуктов Secret Cloud входят: Secret Cloud, Secret Cloud Enterprise, Secret Cloud DRM

Использование баз данных в организациях



Штрафные санкции за утечку данных

SecretTechnologies

152-ФЗ и закон №502104-8

Состав	Было	Стало
Утечка до 100 000 субъектов	100 000–300 000 руб.	3 000 000–5 000 000 руб.
Утечка от 100 000 субъектов	100 000–300 000 руб.	10 000 000–15 000 000 руб.
Повторное нарушение	100 000–300 000 руб.	От 0,1 до 3 % выручки за календарный год, предшествующий нарушению, или за часть текущего года, но не менее 15 000 000 и не более 500 000 000 рублей

SecretTechnologies

Основная работа всех систем происходит с информацией, которая хранится в базах данных

Традиционная инфраструктура

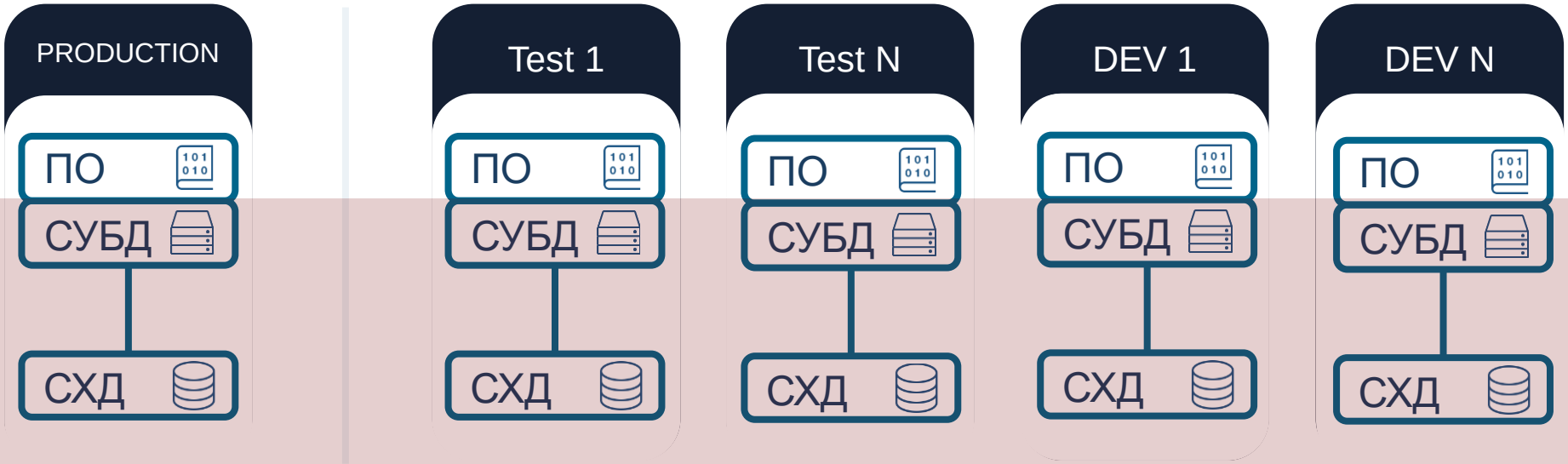
SecretTechnologies

Риск утечки данных

Затраты на защиту

Продуктивная среда

Непродуктивные среды



Реальные конфиденциальные данные

20%

Продуктивные данные

80%

Непродуктивные данные

Данные в непродуктивной среде – основной риск утечки

SecretTechnologies

Непродуктивные данные:

Представляют собой большую зону риска

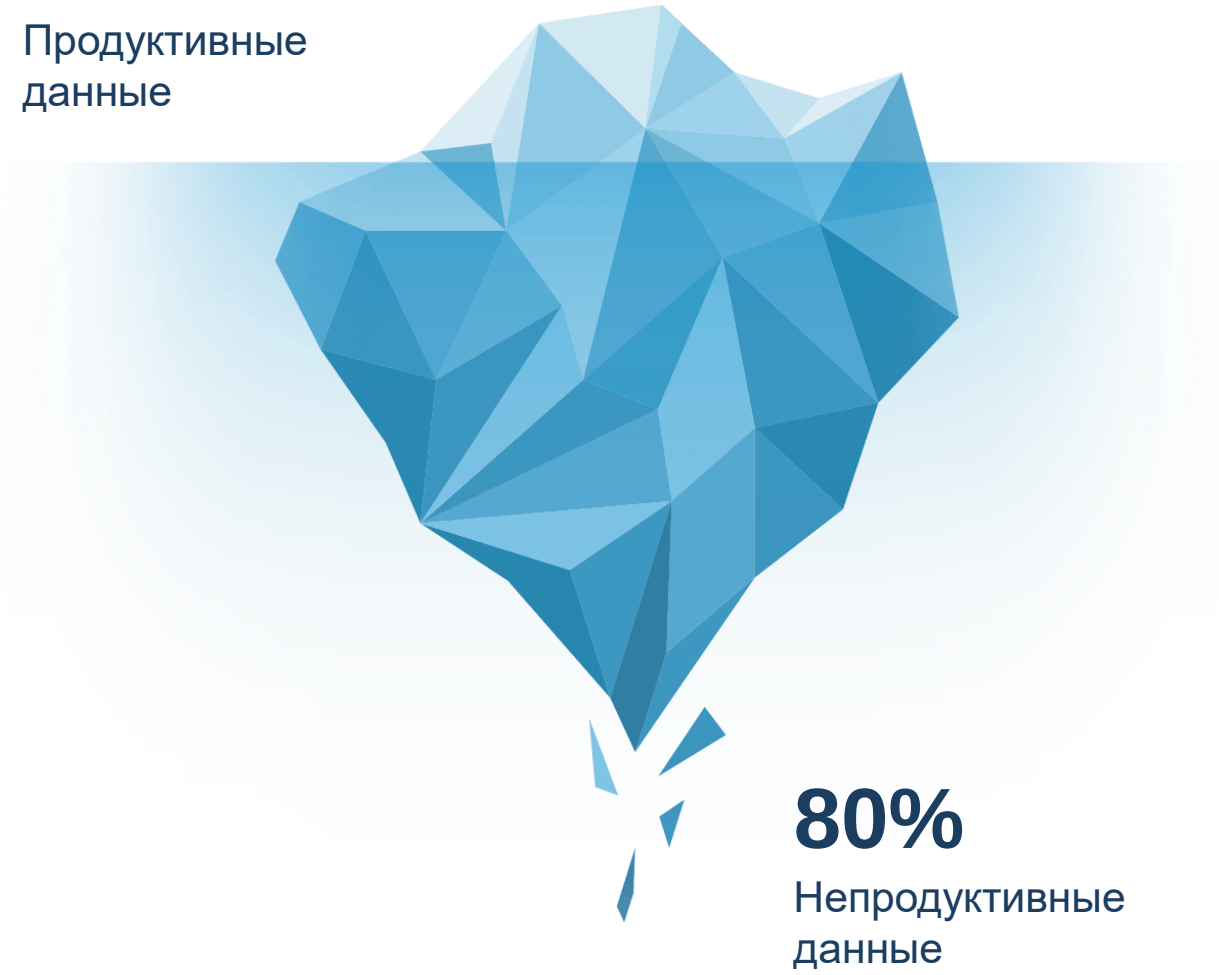
В среднем 8-12 копий для каждого продуктивного источника

Приводят к появлению разрозненных источников данных

Источники защищены множеством инструментов и процессов

Постоянно растут

И со временем меняются



Зачем нужно обезличивание: проблемы и риски при передаче БД

SecretTechnologies

Передача исходной базы

- Несанкционированный доступ
- Случайные утечки из-за человеческого фактора
- Злоумышленные действия инсайдеров
- Нарушение конфиденциальности клиентов
- Финансовые и репутационные риски
- Доступ внешних разработчиков к реальным данным

Синтетическая база

- Длительный процесс генерации
- Отвлечение ресурсов от основных задач
- Нарушение логических связей между данными
- Ошибки в форматах и типах данных
- Недостаточное разнообразие синтетических данных
- Неожиданное поведение системы на реальных данных
- Пропуск критических сценариев при тестировании

Самописные скрипты

- Необходимость адаптации под каждый тип БД
- Сложность реализации комплексных алгоритмов обезличивания
- Трудности с сохранением статистических свойств данных
- Отсутствие гарантий качества обезличивания
- Риск ошибок при написании и обновлении скриптов
- Отсутствие документации и стандартизации

SecretTechnologies

Использование профессионального ПО для маскирования данных - эффективный способ минимизации рисков утечки

Преимущества использования специализированного ПО для маскирования

SecretTechnologies

Надежность и безопасность

- Проверенные алгоритмы маскирования
- Соответствие стандартам и нормативам

Универсальность

- Поддержка различных типов баз данных и форматов
- Возможность настройки под специфические требования

Простота использования

- Предустановленные шаблоны и политики маскирования
- Возможность быстрого развертывания

Эффективность

- Быстрая обработка больших объемов данных
- Автоматизация процессов маскирования

Экономическая эффективность

- Снижение затрат на разработку и поддержку собственных решений
- Уменьшение рисков финансовых потерь от утечек данных

Сохранение целостности данных

- Поддержание целостности
- Сохранение статистических свойств данных

SecretTechnologies

DATA MASK

Отечественное решение по маскированию данных, которое автоматически обнаруживает и видоизмененяет конфиденциальную информацию, содержащуюся в базах данных, предотвращая её несанкционированное использование как внутренними, так и внешними пользователями.

Это позволяет компаниям соблюдать требования законодательства о защите персональных данных и снижать риски утечек чувствительной информации.

Когда применяется маскирование данных

SecretTechnologies

Соблюдение регуляторных требований

При работе с персональными данными клиентов маскирование помогает выполнять законодательные нормы по защите информации.

Предотвращение утечек

При получении злоумышленником доступа к базам данных, маскирование не позволит извлечь реальную информацию из них.

Аутсорсинг

В случае когда данные передаются внешним подрядчикам, маскирование необходимо для обеспечения конфиденциальности информации при её обработке третьими лицами.

Разработка и тестирование

В тестовых средах небезопасно использовать реальные данные, при этом важно сохранить их структуру для минимизации ошибок при разработке ИТ-продукта.

Маскирование данных позволяет сохранить логику представления данных в базе без риска раскрытия конфиденциальной информации.

Аналитика данных

При масштабном анализе данных важно обеспечить анонимность, сохраняя при этом статистическую ценность информации.

Маскирование данных с Data Mask

SecretTechnologies

РЕАЛИСТИЧНОСТЬ

НЕОБРАТИМОСТЬ

ЦЕЛОСТНОСТЬ

ОДНОРОДНОСТЬ

Маскирование всех источников

- Одинаковые правила и алгоритмы

Целостное маскирование

- Одинаковое маскирование всех источников

Различные алгоритмы маскирования

- По словарю с учетом того, от какого лица, пола, формулировки в документе
- Посимвольная замена
- На основе контрольных знаков (ИНН, ОГРН и пр.)
- Уникальные алгоритмы маскирования «под клиента»
- Замена чувствительных данных на константу

Пример алгоритма маскирования

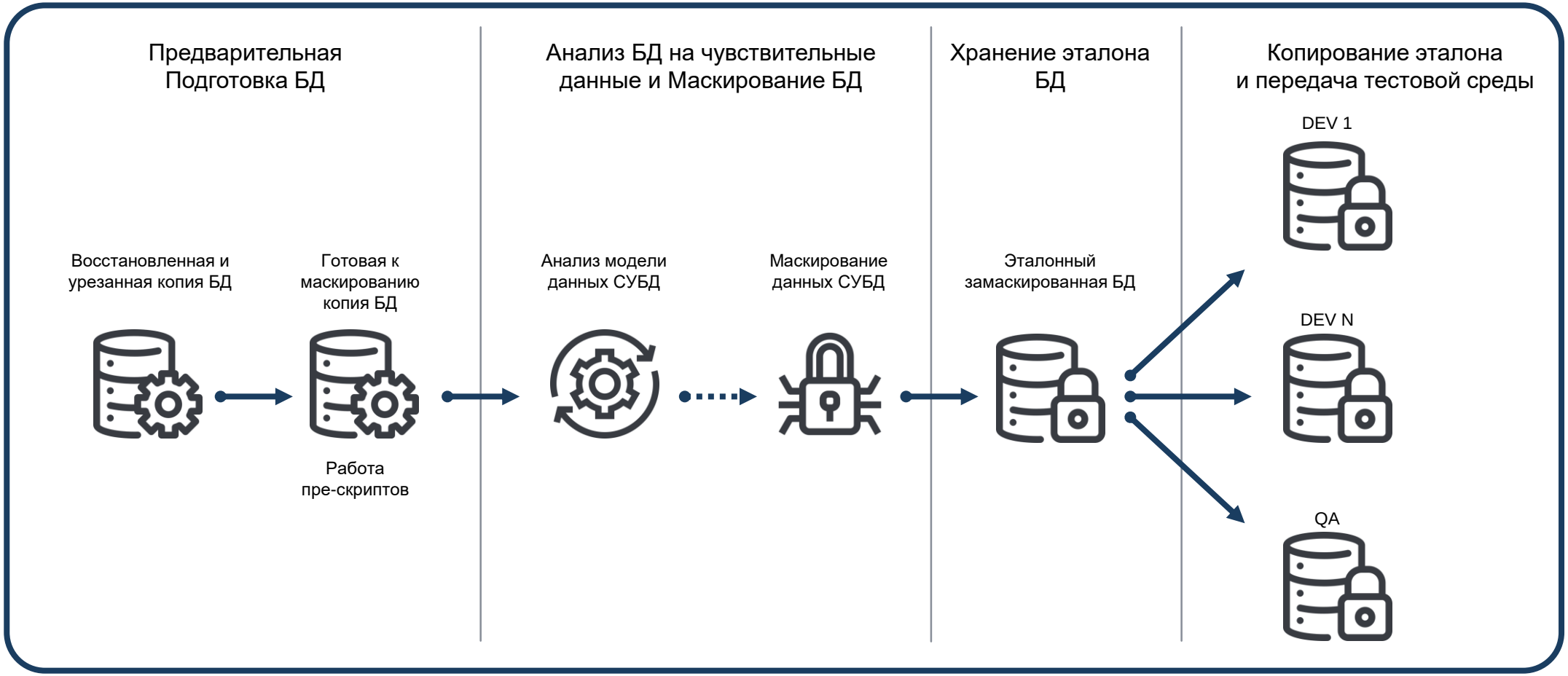
SecretTechnologies

Метод маскирования	В продуктовой базе	В замаскированной копии
По словарю с учетом того, от какого лица, пола формулировки в документе	Марина Антоновна butkova@company.ru	Ирина Артемовна kondashova@so.com
Посимвольная замена	+7 (917) 543 12 32 X235OУ 797	+7 (917) 443 23 98 X001AM 797
На основе контрольных знаков (ИНН, ОГРН и пр.)	771855191856 10388714561	771898383760 10332873218

Процесс предоставления тестовых сред с учетом маскирования данных

SecretTechnologies

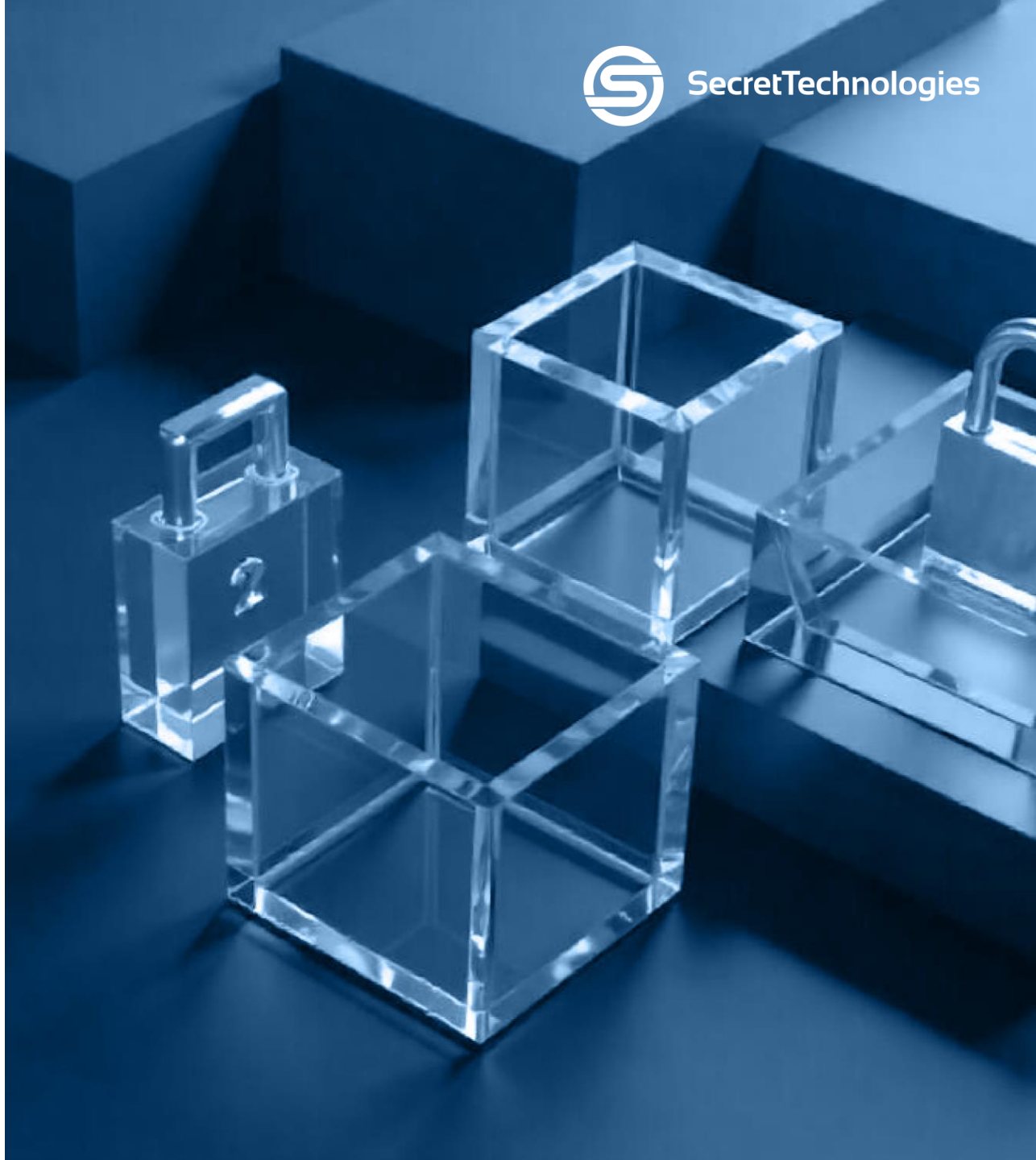
Этапы формирование тестовых сред (ТС) с учетом маскирования



Полный цикл создания ТС при актуализации БД до состояния продуктива

Преимущества Data Mask

- Возможность одновременной обработки различных баз данных в рамках одного процесса
- Запуск маскирования как в ручном, так и в автоматическом режиме
- Предпросмотр результатов маскирования и тестовый прогон процесса обезличивания по колонке
- Возможность миграции данных из одного типа СУБД в другой
- Уникальная схема маскирования для каждого заказчика
- Ускорение работы системы за счет параллельного обезличивания одной таблицы
- Поддержка большого количества СУБД: Postgres, Oracle, MS SQL, Maria DB, и др.
- Консистентность замаскированных данных из разных СУБД в рамках одного заказчика



Тестирование Data Mask*

Встреча в формате ВКС

- Демонстрация ключевых возможностей решения
- Обсуждение ваших потребностей и задач
- Ответы на вопросы в реальном времени

Пилотный проект

- Адаптация под ваши политики безопасности
- Учет особенностей вашей базы данных
- Практическое тестирование в вашей среде

**Для организации встречи и обсуждения пилотного проекта обращайтесь к вашему менеджеру в компании Secret Technologies*