Data Governance, анализ данных и инструменты обезличивания для защиты данных

Решения Informatica

Василий Хасанов
Руководитель направления Data Security

Data 3.0 – тренды 2020

Бурный рост объемов данных

15.3 zettabytes в год
трафик глобальных дата центров

Новые пользователи

325 миллионов
новых бизнес пользователей работающих с данными (и постоянный рост)

Новые типы данных

(mobile, social, IoT)

20 миллиардов
Подключенных устройств

Данные в Cloud

Более 92% трафика дата центров
будут приходится на Cloud

Machine Learning/AI

1 миллиард сотрудников
будут пользоваться помощью machine learning или AI

DIS GROUP

Утечки данных в РФ в 2017 году*

254
Публичных случая

14%
Рост количества утечек по сравнению с 2016

**По материалам Аналитического центра InfoWatch, методология основана на анализе публичных сообщений в открытых источниках*

Распределение утечек по вектору воздействия*

86,3%
Внутренний нарушитель

13,7%
Внешние атаки

**По материалам Аналитического центра InfoWatch, методология основана на анализе публичных сообщений*

Группы риска

Внешние разработчики и тестировщики (подрядчики, аутсорс)

Внешние службы поддержки

Собственные админы и поддержка

Собственные сотрудники

Сложности с проверками и контролем

Требуется работа с данными

Высокий риск утечки

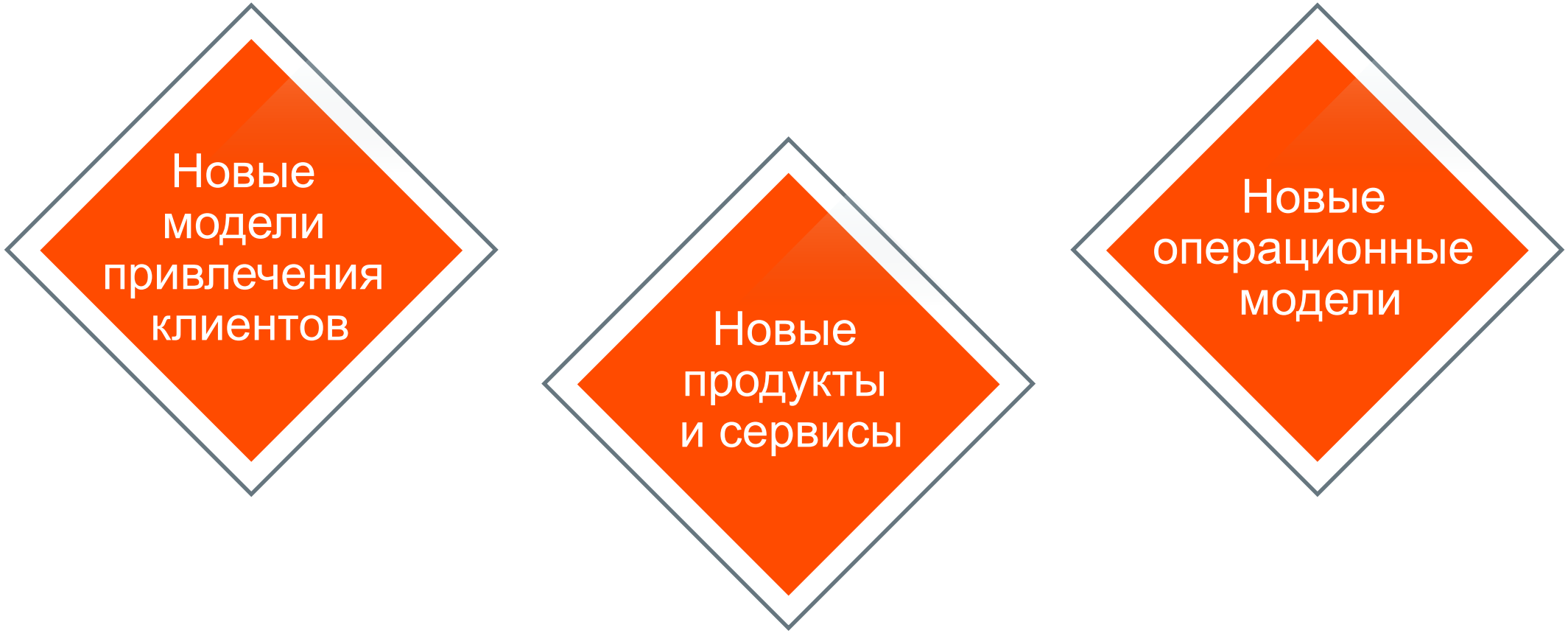
Compliance

Внешние и внутренние регулятивные требования

Российская Федерация	Законодательство о персональных данных, банковской тайне, коммерческой тайне, антитеррористическое законодательство, подзаконные акты, приказы и письма Роскомнадзора, ЦБ и т.п.
Внутренние требования организации	Внутренние требования организации в области обеспечения конфиденциальности и защиты данных
Международные и зарубежные	Множество документов в каждой юрисдикции, наиболее яркий пример последнего времени - General Data Protection Regulation (GDPR) в Евросоюзе (штрафы до 20 млн евро и 4 % оборота)

DIS GROUP

Цифровая трансформация



Данные – основа цифровой трансформации

DIS GROUP

Data Governance

Управление данными для максимальной эффективности бизнеса

Цифровая трансформация: данные - один из важнейших активов организации

Данные – основа для повышения эффективности бизнеса и снижения издержек

Данными нужно эффективно управлять на всех этапах их жизненного цикла

Взаимодействие: Люди – Процессы – Информационные Технологии

Качество данных

Доступность данных для использования во всей организации
с должным уровнем обеспечения безопасности и конфиденциальности

DIS GROUP

Современная проблематика Data Privacy и Data Security

Широкое распространение данных на Enterprise-уровне, рост доступности данных для эффективности бизнеса	Внешние и внутренние регулятивные требования (compliance)	Традиционный фокус на защите периметра, меньше внимания происходящему внутри	Data Governance “на бумаге” и не поддерживается технологиями

DIS GROUP

Data Governance: определение и управление политиками

Informatica Axon Data Governance

Управление политиками конфиденциальности

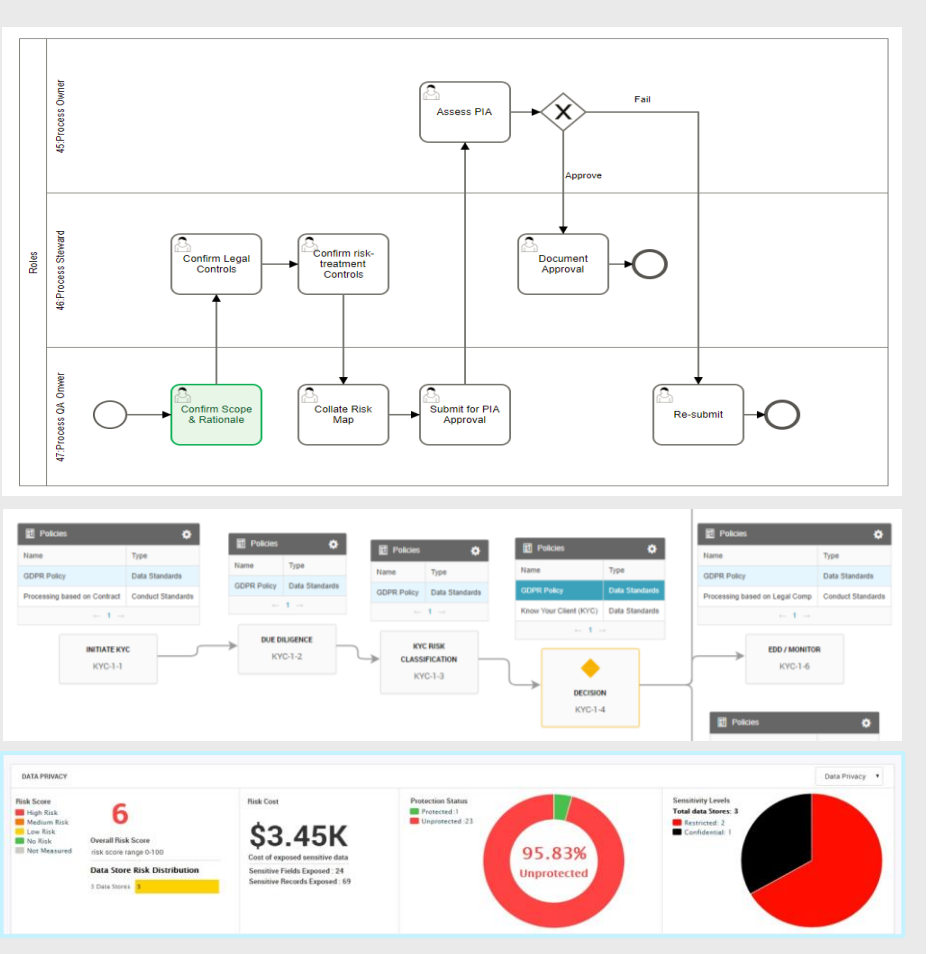
- Определение конфиденциальных и чувствительных данных
- Совместная работа
- Назначение владельцев и ответственных
- Документирование процессов
- Согласование документов

Маппинг политик, business и data контекста

- Инвентаризация бизнес-процессов, использующих конфиденциальные данные
- Маппинг систем и процессов для конфиденциальных данных
- Визуализация результатов процессов обеспечения конфиденциальности и защиты в контексте

Мониторинг и отчетность (compliance)

- Отчетность о результатах для заинтересованных участников
- Инициирование и управление изменениями для оптимизации результатов
- Аудит для всех задействованных артефактов



Знания о реальных данных для эффективной защиты

Какие данные являются конфиденциальными, каков их уровень конфиденциальности?
Подпадают ли эти данные под какое-либо внутреннее или внешнее регулирование и какие политики применяются для этих данных?
Где именно находятся конфиденциальные данные (в каких системах, где именно внутри систем)?
Сколько конфиденциальных данных имеется, каков их объем?
Как данные двигаются внутри организации (между системами, регионами, департаментами и т.п.)?
Защищены ли данные?
Сколько пользователей и кто именно имеет доступ к данным?
Кто непосредственно работает с данными?
Соответствуют ли активности по работе с данными ролям пользователей? Являются ли эти активности необычными или подозрительными?

DIS GROUP

Технологический аспект: выявление расположения, классификация и понимание конфиденциальных данных

Informatica Secure@Source

Классификация

- Классификация конфиденциальных данных в соответствии с потребностями организации

Расположение

- Определение политик и сканирование источников данных
- Получение информации о статусе защиты от внешних решений

Распространение (движение между источниками и приемниками)

- Встроенные возможности выявления для интеграционных решений Informatica (PowerCenter, BDM) и сторонних поставщиков (Microsoft, Cloudera, Hortonworks, etc.)
- Возможности загрузки custom данных о распространении

Визуальное информирование и понимание

- Глобальное представление о конфиденциальных и чувствительных данных в организации
- Топ источники, домены, департаменты и т.п.
- Визуализация распространения (движения) данных

DIS GROUP

Анализ риска данных на постоянной основе

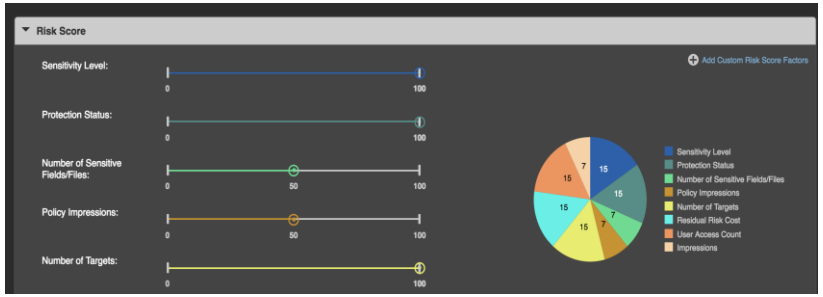
Informatica Secure@Source

Классификация и обнаружение

Политика и уровень конфиденциальности, физическое и логическое расположение

Распространение

Движение данных внутри и снаружи организации



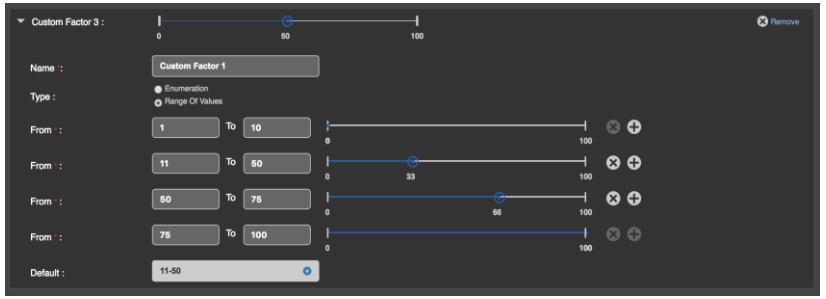
Стоимость утечки

Стоимость последствий утечки данных для организации.

RISK

Объемы данных

Количество записей о конфиденциальных данных

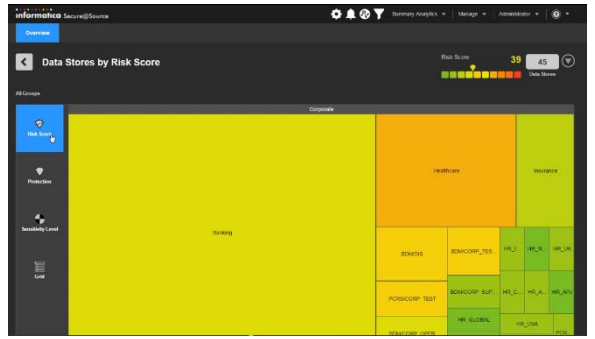


Доступ и активность пользователей

Частота и интенсивность пользовательской активности

Защита

Защищены ли данные



Custom Риск-Факторы

Создание и мониторинг дополнительных custom факторов в соответствии с потребностями организации

DIS GROUP

Действия по защите и минимизации рисков

Informatica Secure@Source

Выявление

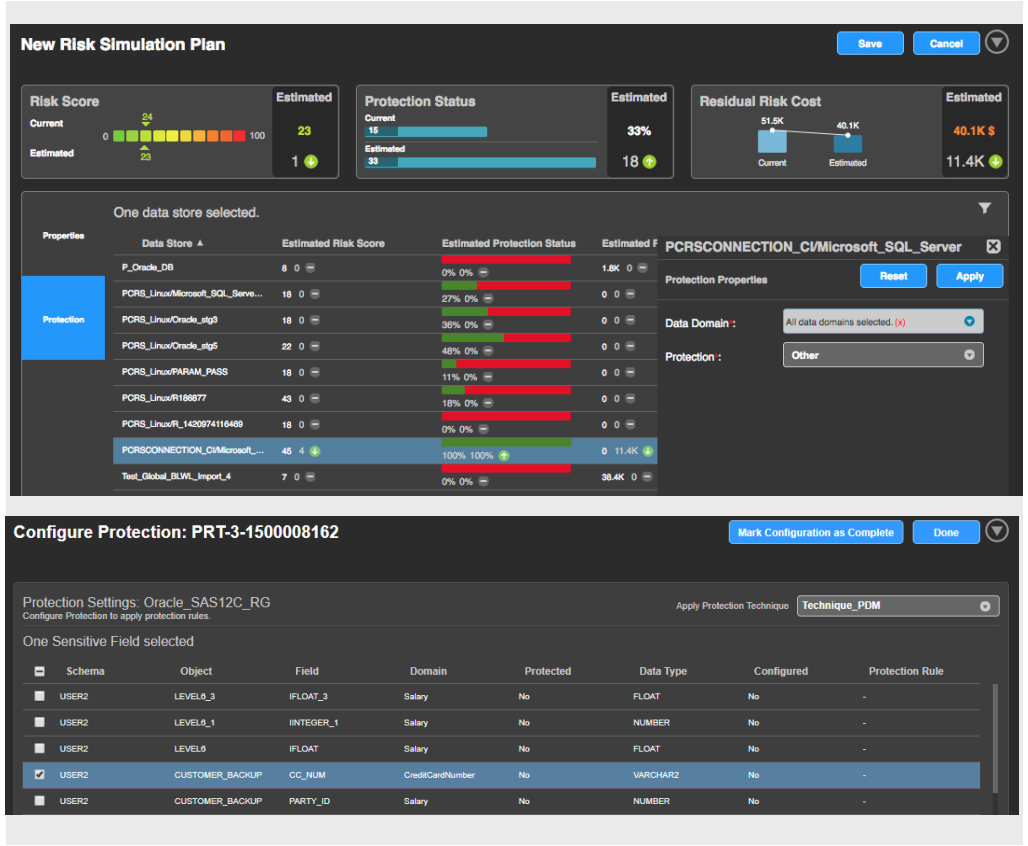
- Незащищенные конфиденциальные данные высокого риска

Ответные действия и Защита

- Защита данных средствами обезличивания Informatica
- Защита данных средствами Ranger и Sentry
- Инициирование действий в инструментах защиты сторонних производителей: шифрование, тикет-системы (ServiceNow), системы контроля доступа и токенизации

Операционная деятельность

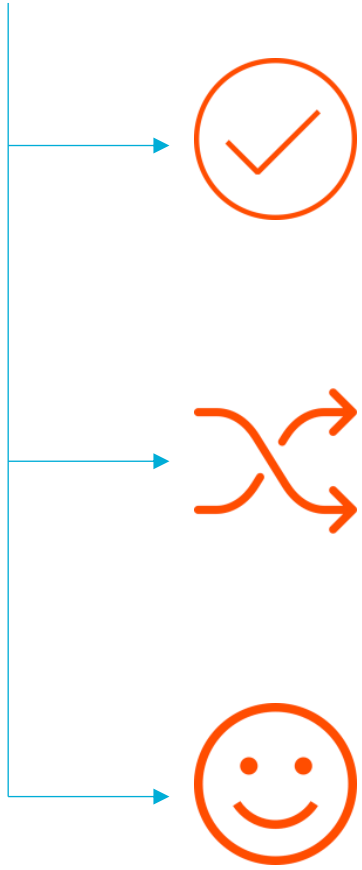
- Автоматизация действий по снижению рисков
- Статус процессов минимизации рисков
- Работа с оповещениями



DIS GROUP

Informatica
для обезличивания (маскирования) данных

Обезличивание (маскирование) данных



Эффективный способ защиты конфиденциальной информации

Замена реальных данных фиктивными данными

Статическое (persistent) обезличивание – изменение данных в БД

Динамическое (dynamic) обезличивание – изменение данных при отображении

Сохранение возможности работы с данными

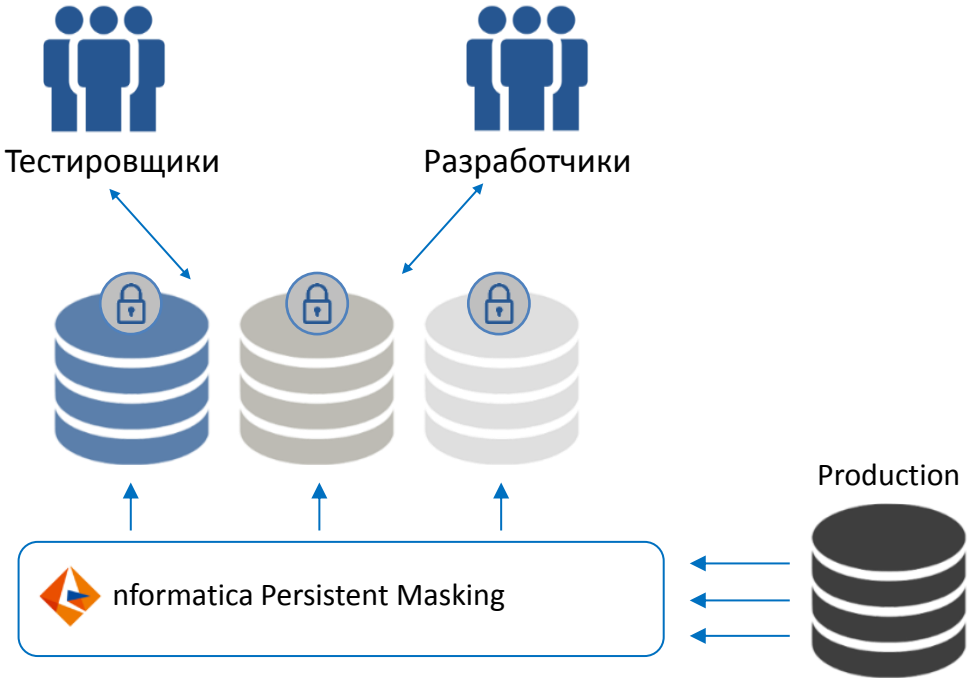
DIS GROUP

Методы обезличивания Informatica

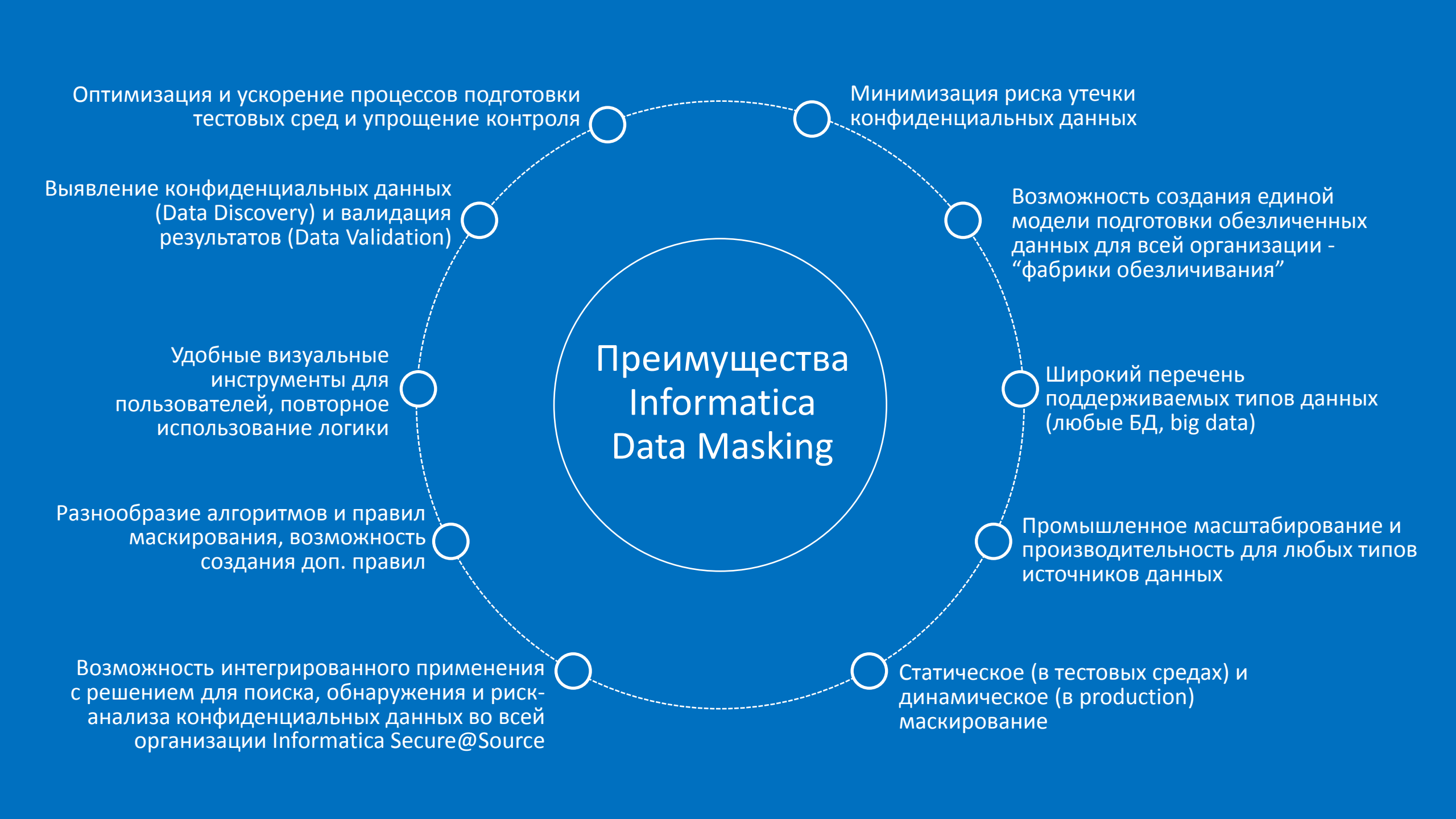
Динамическое обезличивание
для работы с данными Prod

- Маскирование критичных данных для неавторизованных пользователей
- Приложения и данные в БД не меняются
- Изменяется представление а не сами данные

Статическое обезличивание
для Test/Dev окружений



- Фиктивные данные для целей тестирования
- Критичные данные полностью изменяются на постоянной основе
- Полное исключение риска доступа к критичным данным


Преимущества Informatica Data Masking
Оптимизация и ускорение процессов подготовки тестовых сред и упрощение контроля
Минимизация риска утечки конфиденциальных данных
Выявление конфиденциальных данных (Data Discovery) и валидация результатов (Data Validation)
Возможность создания единой модели подготовки обезличенных данных для всей организации - “фабрики обезличивания”
Удобные визуальные инструменты для пользователей, повторное использование логики
Широкий перечень поддерживаемых типов данных (любые БД, big data)
Разнообразие алгоритмов и правил маскирования, возможность создания доп. правил
Промышленное масштабирование и производительность для любых типов источников данных
Возможность интегрированного применения с решением для поиска, обнаружения и риск-анализа конфиденциальных данных во всей организации Informatica Secure@Source
Статическое (в тестовых средах) и динамическое (в production) маскирование

3 из 3

крупнейших банков РФ по
размеру активов

успешно обезличивают данные
для тестовых сред
с помощью Informatica

Informatica для Data Privacy и Data Security

Обнаружение рисков конфиденциальных данных

Бизнес-классификация, инициативы Data Governance	Техническая классификация, анализ данных и их распространения, оценка риска	Планирование защиты и действий по снижению рисков

Динамическое обезличивание Real-time Masking Бизнес-Приложения	Шифрование Data Encryption Базы Данных	Статическое обезличивание Persistent Masking Аналитика, DevOps

Защита данных и приложений

DIS GROUP

DIS GROUP

Спасибо за внимание!

+7 (495) 645 02 01

info@dis-group.ru