ЭВРИТЕГ
Платформа
Безопасности
Данных

ЭВРИТЕГ

О компании

Лидер на российском рынка среди решений по предотвращению утечек чувствительных данных

С 2014 года внедряет решения в области информационной безопасности и управления корпоративным контентом. Является владельцем запатентованной технологии маркировки электронных документов различного формата.

Модуль маркировки для СЭД, почты и печати

Инструменты для проведения экспертизы и выявления источника утечки конфиденциальных данных из систем документооборота компаний

Виртуальная комната данных

Хранилище для удобного и безопасного обмена документами и файлами и совместной работы с управлением доступа к файлам и папкам

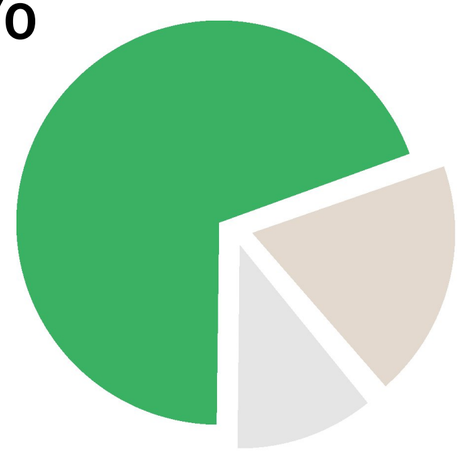
Платформа Безопасности Данных

Комплексное решение для управления доступом к конфиденциальным данным, с высоким уровнем защиты от хакеров и неправомерных действий пользователей

Статистика утечек

Источники утечки информации

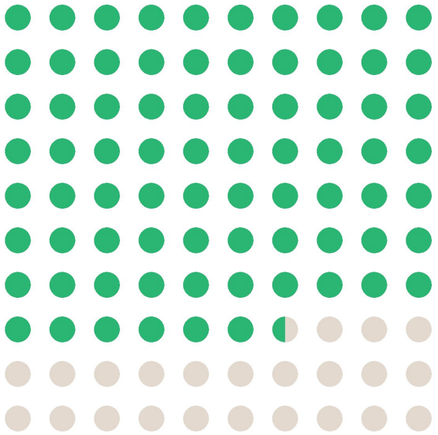
70,1%
Внешние угрозы



19,1%
Инсайдеры

10,8%
Другое

Форматы утечек



85,5%
Digital каналы

14,5% Фото и бумажные копии, другие каналы

Утечки из баз данных

1,5 млрд
записей личной информации пользователей РФ украдено за 2024 год

6,9% конфиденциальной информации происходит через мессенджеры, где чаще всего можно обнаружить фото и скриншоты чувствительных документов

*по данным отчета InfoWatch 2025

Ответственность за массовые утечки персональных данных станет существенной

Оборотные штрафы

от 3 000 000 до 15 000 000 руб.
в первый раз

штрафы за утечку от 1000 субъектов персональных данных (то есть граждан) для юрлиц

до 3% выручки за год за повторное нарушение

или за часть текущего года, но не менее 15 млн руб. и не более 500 млн руб.

Косвенные экономические потери

Снижение продаж и ухудшение конкурентного положения

Репутационный ущерб

Снижение лояльности и потеря клиентов

При текущих подходах в ИБ основные причины утечек невозможно устранить

Получение хакерами доступа к инфраструктуре через эксплуатацию ее уязвимостей и компрометацию учётных данных пользователей

Утечка дампа базы или файлов данных вследствие умышленных действий администраторов или нарушения регламентов эксплуатации серверной инфраструктуры

Выгрузка данных за счёт автоматизации запросов вследствие умышленных действий пользователя или кражи его учётных данных

Требуется 6 и более СЗИ с разными интерфейсами и крайне высокая квалификация у ИТ и ИБ подразделений

ЭВРИТЕГ Платформа безопасности данных

Комплексное решение для управления доступом к конфиденциальным данным, обеспечивающее высокий уровень защиты от хакеров, а так же от ошибочных или неправомерных действий привилегированных пользователей.

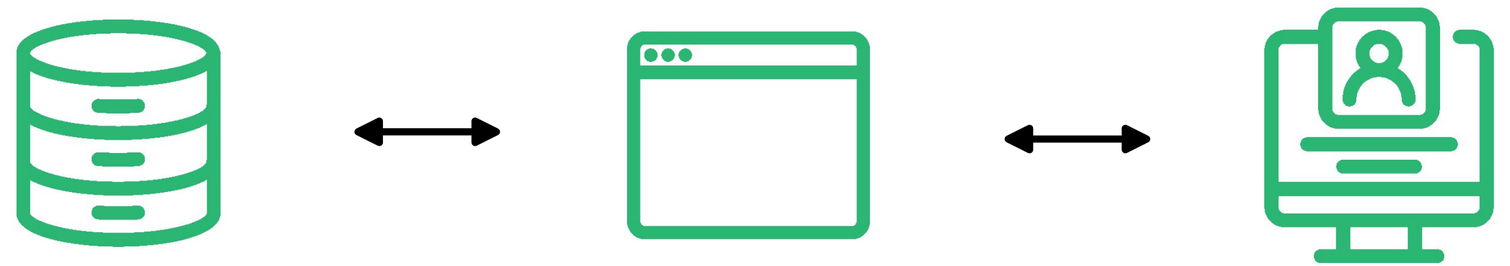
Эти аспекты возможны благодаря ключевым принципам платформы:

Открытая архитектура на принципах нулевого доверия

Публичная программа кибериспытаний

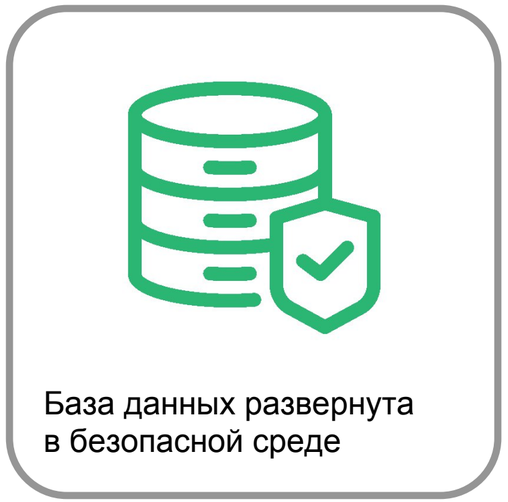
Агент для контроля серверов баз данных с открытым исходным кодом

Стандартная схема работы с базами данных



- уязвима на уровне клиента и бизнес-приложения
- уязвима со стороны привилегированных пользователей
- уязвима на уровне инфраструктуры

Изолируем базу данных в безопасной среде

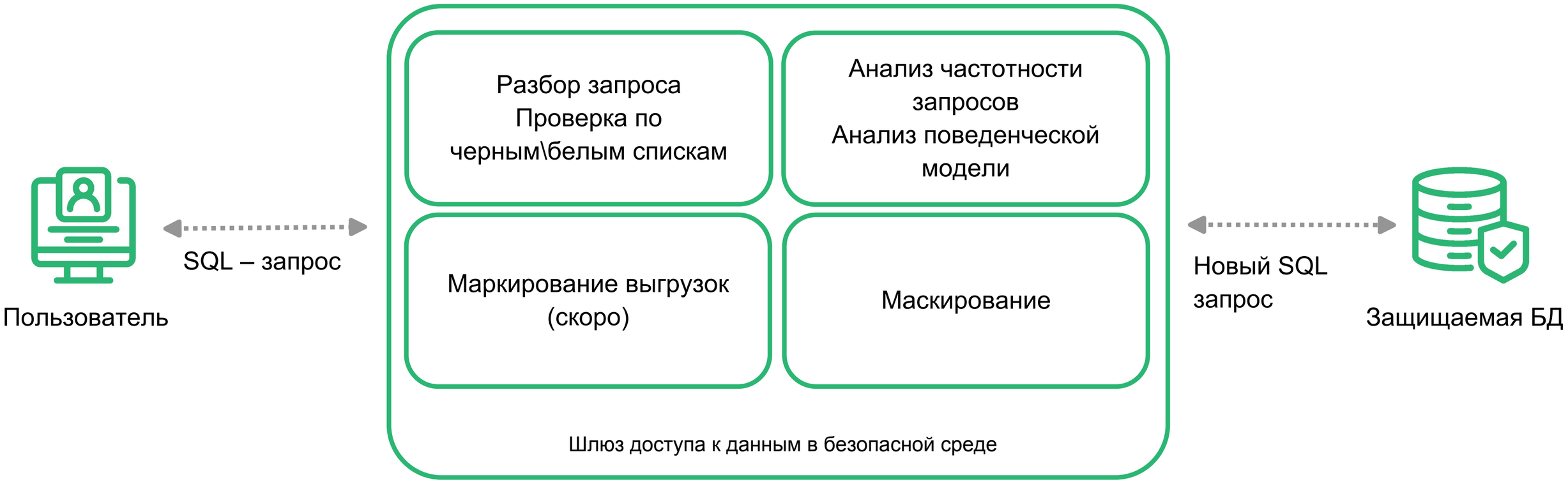


– уязвима на уровне клиента и бизнес-приложения
✓ защищена со стороны привилегированных пользователей
✓ защищена на уровне инфраструктуры

Контролируем запросы к данным

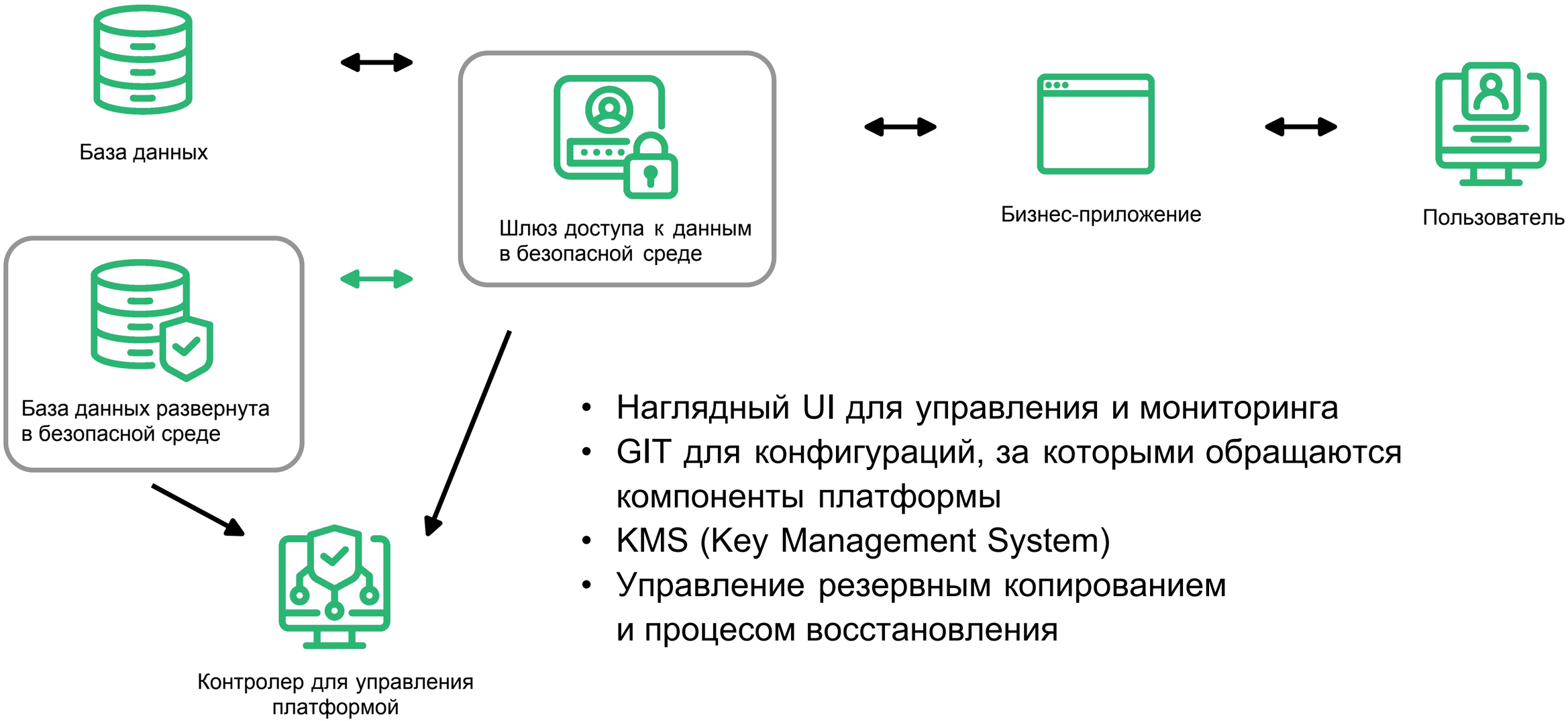
- ✓ защищена на уровне клиента и бизнес-приложения
- ✓ защищена со стороны привилегированных пользователей
- ✓ защищена на уровне инфраструктуры

Способы контроля доступа к данным



Новый SQL запрос от шлюза доступа к данным с подготовленными выражениями, которые отделяют данные от SQL команд, предотвращая SQL инъекции

Даем инструменты для управления и наблюдения



- Наглядный UI для управления и мониторинга
- GIT для конфигураций, за которыми обращаются компоненты платформы
- KMS (Key Management System)
- Управление резервным копированием и процесом восстановления

Три сценария использования платформы

Сценарии могут быть применимы в любом сочетании, в том числе и одновременно, что обеспечивает гибкость и адаптивность решения к потребностям бизнеса

1.

Фильтрация всех SQL запросов к базе данных. Ответственность за конфигурацию и защиту сервера БД лежит на ИТ и ИБ специалистах.

2.

Изоляция СУБД, контроль соответствия политикам безопасности и фильтрация всех SQL запросов к базе данных. Усиление защиты за счёт контроля сетевого доступа и соблюдение политик безопасности.

3.

Запуск баз данных в безопасной среде исполнения и контроль политик выгрузки данных. Режим максимальной защиты для особенно чувствительной информации.

Преимущества платформы для клиентов

Защита баз данных даже при полном доступе хакеров к инфраструктуре

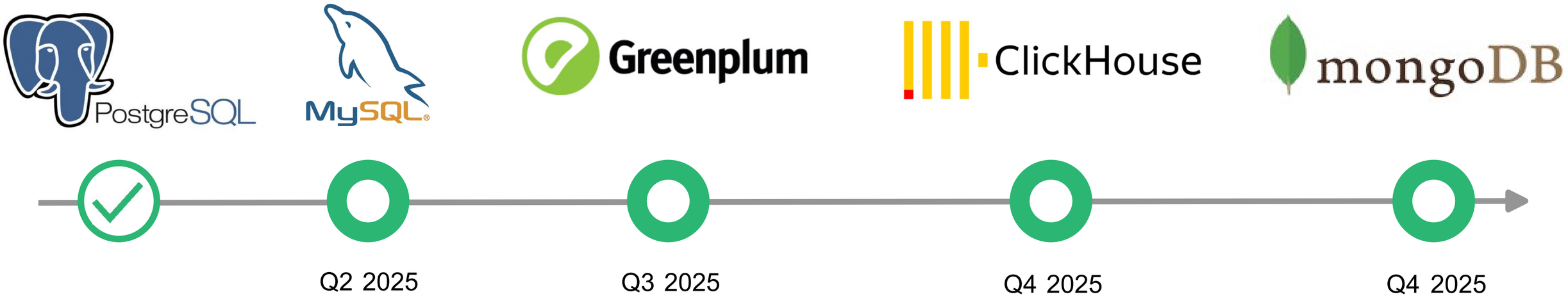
Предотвращение несанкционированного доступа к данным, включая действия недобросовестных сотрудников

Легкая интеграция с существующими приложениями без необходимости вносить изменения в код

Масштабируемость и сохранение данных даже при технических сбоях или человеческих ошибках благодаря применению безопасного шифрования

Удобное управление, не требующее специальных навыков

Поддерживаемые СУБД



Поддержка Oracle и других SQL баз данных может быть рассмотрена в рамках отдельного спец. проекта

Забронируйте онлайн демо

EVERYTAG.RU/DSP

EVERYTAG.RU +7 (495) 141 44 45 sales@everytag.ru

Функциональные возможности платформы

Управление доступом ко всем базам данных компании без агента \ с применением агента

Развертывание баз данных в безопасной среде

Преднастроенные политики безопасности, которые можно адаптировать под конкретную специфику бизнеса

Возможно масштабировать под любую нагрузку и резервировать для отказоустойчивости

Удобные инструменты для аудита использования данных

Специально разработано для корпоративных облаков (cloud native)