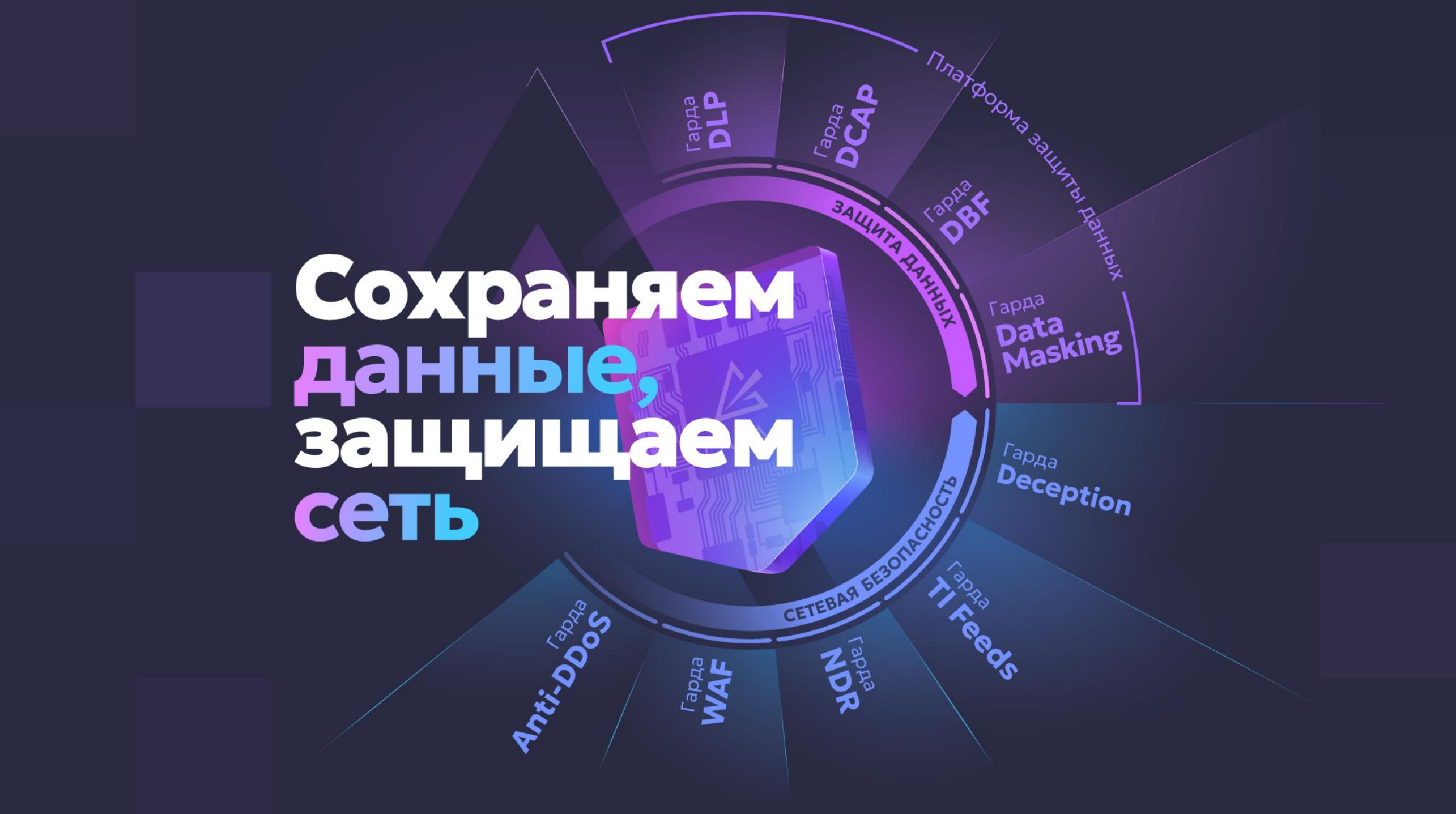
Сохраняем данные, защищаем сеть




NDR + DBF
Как ловить тихую
эксфильтрацию из БД
в зашифрованном трафике

Типовые сценарии «тихой» утечки

- Взлом веб-приложения. Злоумышленник использует легитимный пул соединений с БД
- Компрометация аккаунта администратора или разработчика, который имеет доступ к прод-БД
- Внутренний инсайдер выкачивает данные маленькими частями
- Внутренний инсайдер создает копию данных скриптами

Что дает Гарда NDR:

- Видимость сетевых потоков между серверами приложений и БД
- Мониторинг сетевых потоков внутри инфраструктуры и при взаимодействии с внешними ресурсами
- Видимость подозрительных событий
  VPN-подключения, подозрительные хосты, сканирование, malware и т.д.

Что дает Гарда DBF:

- Классификацию объектов БД: чувствительные таблицы, ПДн, финансы.
- Видимость доступов к информации в БД
- Видимость зашифрованного трафика : TLS, HTTPS
- Блокировку запросов к БД в реальном времени

Часто данные из БД утекают от внутреннего злоумышленника — как это обнаружить и заблокировать?

3 шага к обнаружению тихой эксфильтрации

Полезные приемы

Определить, что именно считается утечкой

Если вы не знаете, какие таблицы для вас критичны, то любая эксфильтрация для системы будет выглядеть как обычный SELECT

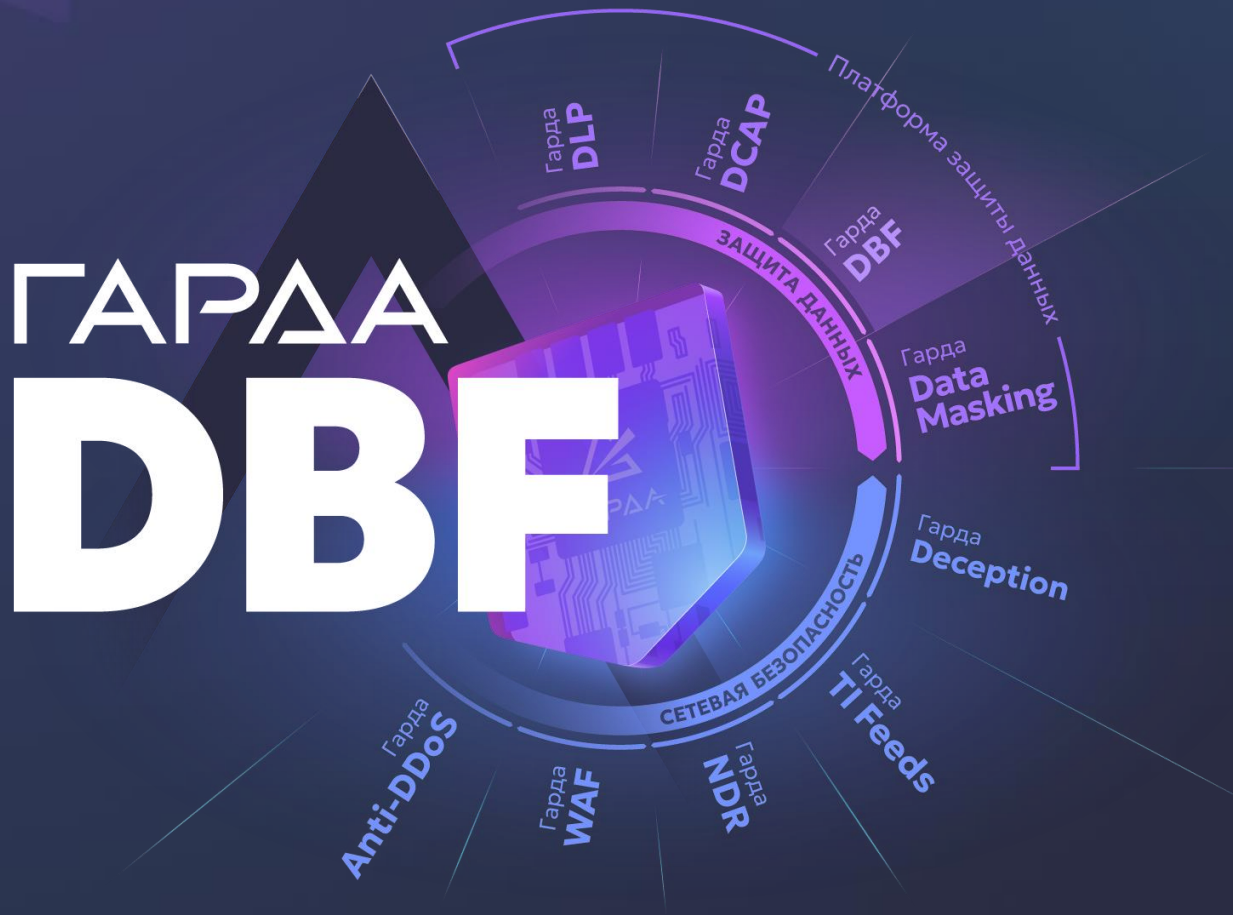
Построить «нормальный» профиль поведения

Без поведенческой модели в БД вы будете ловить только грубые и шумные атаки.

Интегрируем DBF и NDR

Тихую эксфильтрацию мы ловим не одним супер-сигнатурным правилом, а связкой слабых сигналов.

Гарда DBF защищает базы данных из единого центра управления



- Отслеживает операции с базами данных и бизнес-приложениями
- Использует поведенческую аналитику для выявления отклонений
- Поддерживает гибкие правила реагирования: при обнаружении аномальной активности может автоматически заблокировать доступ или попытку вмешательства извне
- Позволяет контролировать действия привилегированных пользователей и выявлять факты сокрытия следов несанкционированной активности

ГАРДА

Записаться на демо Гарда DBF

Офис в Москве

БЦ «SkyLight», Ленинградский проспект д. 39, корп 80,
Башня Б, 18 этаж

8-800-770-70-60

info@garda.ai

Спасибо за внимание!

Сохраняем данные, защищаем сеть