

# Гарда DBF

## Комплексная защита и аудит баз данных

Решение обеспечивает полный контроль операций в базах данных и бизнес-приложениях. Выявляет внешние атаки и злоупотребления привилегиями в реальном времени, блокирует несанкционированную активность до нанесения ущерба.

## С Гарда DBF вы сможете



Находить и классифицировать все базы данных в компании



Сканировать СУБД на уязвимости



Проверять конфигурацию баз данных на соответствие требованиям регуляторов



Контролировать операции с данными и действия пользователей (в т. ч. привилегированных)



Выявлять вмешательство в работу СУБД извне или инсайдерскую активность



Блокировать подозрительные запросы, нелегитимное повышение прав и попытки кражи данных

## Функциональные возможности

### Аудит СУБД и данных

- **Классификация данных.** Находит и помечает персональные, финансовые, учетные и другие конфиденциальные данные
- **Проверка уязвимостей.** Информировать о неустановленных обновлениях, выявляет небезопасные настройки, слабые пароли, дефолтные учетные записи, даёт рекомендации по исправлению
- **Анализ привилегий.** Показывает, кто и к чему имеет доступ; находит избыточные права и нарушение принципа минимальных привилегий

### Ретроспективный анализ

- **Восстанавливает картину событий:** кто, что, когда изменил, какие данные выгрузил
- **Предоставляет контекст событий** и другие артефакты для расследований и отчетов регулятору
- **Формирует дашборды** для оперативного анализа, создает отчеты об исправленных конфигурациях

### Поведенческая аналитика (UEBA)

- **Понимание контекста.** Отслеживает активность пользователей, приложений и сервисных учетных записей
- **Аномалии и риск.** Обнаруживает нетипичные запросы, нехарактерные выгрузки и другие подозрительные операции. Сигнализирует о реальных угрозах
- **Политики реакции.** Ограничивает объём и состав выгружаемых данных, частоту запросов: предупреждение,

### Активное реагирование

- **Блокировка.** Решение приостанавливает подозрительные запросы и доступ к конфиденциальным данным на основе настроенных правил и анализа поведенческих аномалий
- **Управление доступом.** Разграничение прав доступа к СУБД и объектам на основе настроенных политик

# Как работает Гарда DBF

1

Гарда DBF перехватывает SQL-запросы и ответы (включая шифрованный TLS 1.3)\*

2

Выполняет глубокий анализ содержимого, переменных и контекста, сопоставляет с политиками безопасности (сигнатуры, белые/черные списки, поведенческие профили). Опционально подключается UEBA для выявления аномалий на основе поведенческих моделей

3

Выносит вердикт: разрешить, заблокировать или зафиксировать инцидент

4

Все события записываются в неизменяемый журнал аудита с возможностью ретроспективного анализа и отправки в SIEM/SOC/SOAR в реальном времени

5

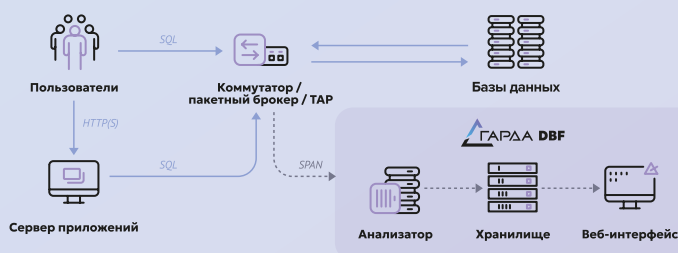
Событие отправляется в модуль автоматических отчетов (опционально)

\* Применимость зависит от схемы перехвата. Требуется консультация инженера Гарды.

## Гарда DBF в инфраструктуре

Предусмотрены три варианта подключения, которые могут комбинироваться в гибридных схемах

### 1. Копия трафика (режим Database Activity Monitoring)



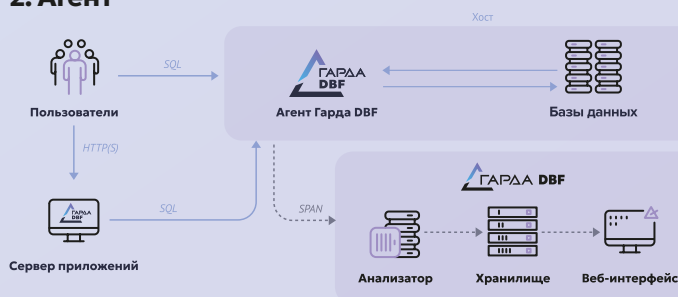
#### Принцип

Пассивный перехват сетевых пакетов на коммутаторе или пакетном брокере без установки агентов

#### Особенности

- Отсутствие влияния на производительность СУБД
- Нет блокировки запросов
- Не контролирует локальные подключения

### 2. Агент



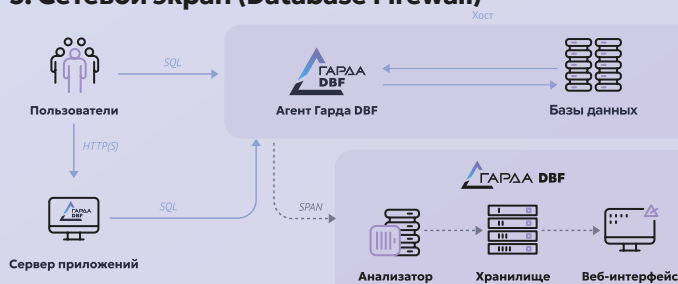
#### Принцип

Программный модуль на хосте с БД, перехватывающий все обращения (сетевые и локальные, включая сокеты)

#### Особенности

- Блокировка нелегитимных действий
- Контроль локальных подключений и изменений файлов
- Подходит для облачных БД (при установке на хост)

### 3. Сетевой экран (Database Firewall)



#### Принцип

Выделенный модуль, работающий в разрыве между клиентами и сервером БД как L3-прокси

#### Особенности

- Полнотекстовый анализ и блокировка без нагрузки на СУБД
- Единственный способ защиты облачных СУБД (DBaaS)
- Не контролирует локальные подключения

# Почему выбирают Гарда DBF



Широкая совместимость: поддержка 40+ СУБД, Big Data, облачных сред



Российское решение, сертифицированное ФСТЭК России



Защита веб-приложений, ERP, CRM и других информационных систем



Снижение комплаенс-рисков. Соответствие требованиям регуляторов и отраслевых стандартов:



Быстрый запуск: 200+ предустановленных политик, решение до 80% типовых задач сразу после установки

- ФЗ-98 «О коммерческой тайне»
- ФЗ-149 «О защите информации»
- ФЗ-152 «О персональных данных»
- ФЗ-187 «О безопасности КИИ»
- ПП РФ № 1119 о защите ПДн
- Приказы ФСТЭК России №117, 21, 31, 239
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций»
- PCI DSS



Поведенческий анализ для выявления мошеннических операций с возможностью их блокировки



Выявление скрытых (теневых) баз данных в инфраструктуре

## Поддерживаемые СУБД

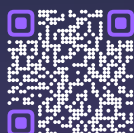
- Oracle
- Microsoft SQL
- MySQL
- SAP HANA
- PostgreSQL
- Teradata
- Sybase ASE
- IBM Netezza
- Линтер
- Apache HBase
- Apache Cassandra
- Hive5
- Ред БД
- SPARK
- Informix
- Sun MySQL
- Apache Kafka
- Vertica
- Greenplum
- ClickHouse
- ArenadataDB
- Квант-Гибрид
- Arenadata QuickMarts
- Arenadata Firebird
- Arenadata Prosperity
- MongoDB
- Interbase
- Jatoba
- Яндекс Database
- IBM DB2
- MariaDB
- Tarantool
- PostgresPro
- ScyllaDB
- SAP Sybase
- 1С Предприятие
- Pangolin
- Tantor
- Tantor SE1C
- Tantor SE
- Redis
- OpenSearch
- SQL Server Analysis Services



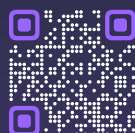
### Что поможет выявить пилот:

- забытые и теневые базы данных
- избыточные права доступа
- подозрительную активность в базах данных
- массовые выгрузки конфиденциальных данных

8 800 770 7060  
**garda.ai**  
info@garda.ai



Закажите  
бесплатный  
пилотный  
проект



Подписывайтесь  
на наш ТГ-канал