ГАРДА БД

Информационная безопасность:
Аудит сетевого доступа
к базам данных и веб-приложениям

ГАРДА БД

«Гарда БД» — аппаратно-программный комплекс класса DAM *(Database Activity Monitoring — система аудита сетевого доступа к базам данных)* выявляет возможные утечки информации и повышает надежность защиты баз данных.

«Гарда БД» — новое поколение интеллектуальной защиты баз данных

Мощные аналитические возможности

Интеллектуальная система хранения данных

Удобство управления

Задачи безопасности решаются с «Гардой БД»

- Повышение уровня защищенности баз данных и веб-приложений:
  - контроль администраторов и привилегированных пользователей;
  - оповещение о попытках доступа (неудачные авторизации к базам данных, ошибки доступа).
- Мониторинг неправомочных обращений к базам данных в режиме реального времени.
- Сканирование и выявление уязвимостей СУБД.
- Хранение всех запросов к базам данных для ретроспективного анализа.
- Обеспечение соответствия требованиям законодательства, отраслевых стандартов и международных соглашений (152-ФЗ «О персональных данных», 161-ФЗ «О Национальной платежной системе», П-1119 «Об утверждении требования к защите ПДн…», Положение Банка России о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств 382-П, PCI DSS, соглашение Basel II, SOX и пр.).

Принцип работы

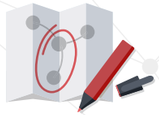
Система «Гарда БД» контролирует все запросы к базам данных и веб-приложениям в режиме реального времени и хранит их в течение длительного срока.

Политики безопасности в реальном времени позволяют выявлять потенциальные инциденты и критичные для компании события.

Технологии нового поколения

Решение «Гарда БД» построено на инновационных технологиях контроля и анализа данных:

интеллектуальная система хранения больших массивов данных



контроль трехзвенной архитектуры без дополнительных затрат на WAF-системы

высокопроизводительный анализ трафика, поиск в 10…100 Тб за секунды

независимость от администраторов, многоуровневый контроль привилегированных пользователей

масштабируемость системы (увеличение производительности и повышение отказоустойчивости для работы с большим числом баз данных в распределённых филиальных сетях)

Функциональные возможности

Обнаружение баз данных

Система автоматически находит новые базы данных в сети компании.

Классификация баз данных

- Сканирование баз данных на наличие конфиденциальной информации, номеров кредитных карт, ИНН и т.п.
- Регулярное отслеживание появления новых баз данных и внесения изменений в имеющиеся.

Сканирование на уязвимости

Тесты уязвимости позволяют определить:

- незаблокированные учетные записи;
- неустановленные патчи;
- учетные записи с простыми паролями;
- активность системных учетных записей других приложений.

Система отчетности

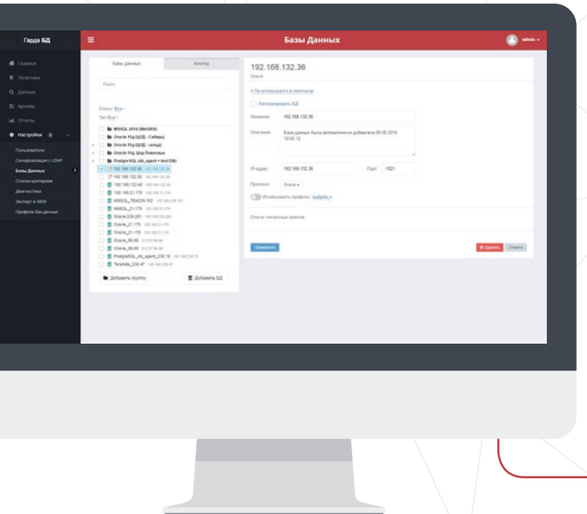
Детализированная отчетность по всем событиям безопасности и операциям пользователей СУБД.

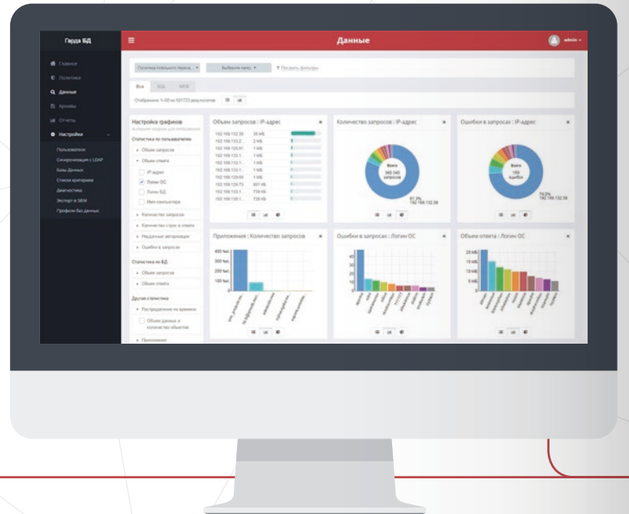
Мониторинг в реальном времени

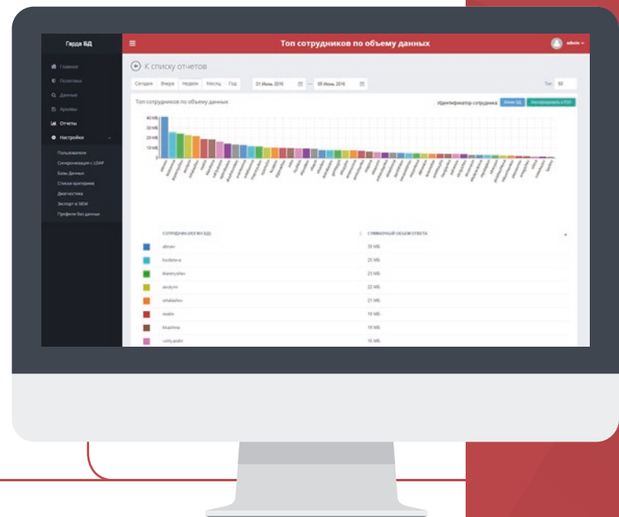
С помощью гибкого конструктора политик безопасности осуществляется контроль всех потенциальных инцидентов (изменение прав пользователя, аномальная активность) для реагирования в реальном времени.

Ретроспективный анализ

Возможность за несколько секунд восстановить и проанализировать информационную картину обмена данными.







Функциональные возможности / продолжение

Интеллектуальные алгоритмы поиска

- Контентный — по запросам, ответам и переменным.
- Атрибутивный — по IP-адресам, учетным записям, текстам ошибок и т. д.

Контроль веб-приложений

- SAP Business Object
- Microsoft Dynamics CRM
- Веб-формы
- Гибкие настройки для работы с любыми бизнес-приложениями на основе HTTP(s)-протоколов

Уведомление о событии

- SIEM
- e-mail
- отчет на главном экране

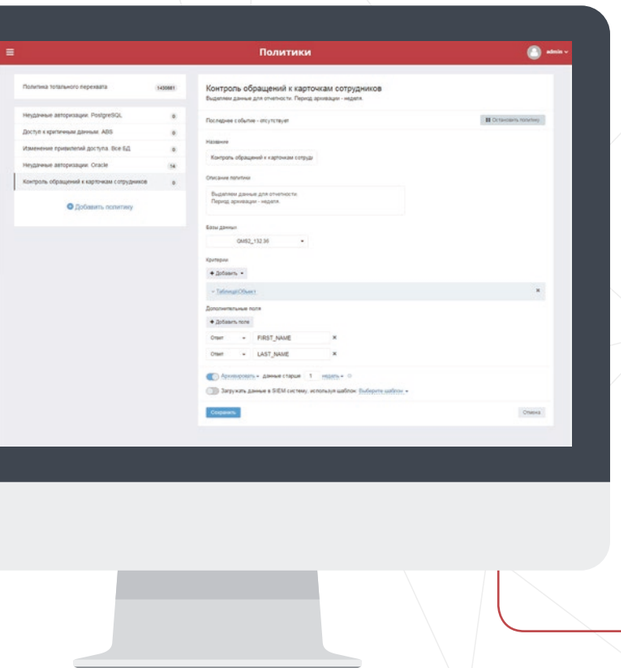
Контролируемые СУБД

- Oracle
- Microsoft SQL
- MySQL
- PostgreSQL
- Teradata
- Sybase ASE
- IBM Netezza
- IBM DB2
- Линтер
- Apache Cassandra

Графическое отображение данных

Понятные графические отчеты позволяют выявить отклонения в статистической картине доступа к базам данных. Интерактивные графики и диаграммы обеспечивают переход к конкретным информационным объектам.

Выявление и расследование инцидентов



Гибкое формирование политик безопасности

- Имя пользователя в БД и имя пользователя в ОС.
- Контроль обращений к регулярным выражениям (номер карты, ИНН и др.).
- Сетевые параметры: ip-адрес (хоста, подсети), порт, диапазон адресов.
- Объем данных ответа.
- Количество записей в ответе.
- Контроль неявных обращений.
- Название используемого клиентского приложения.
- Запрашиваемые/передаваемые поля таблицы, синонима, представления.
- Ключевое слово (поиск в запросах, ответах и переменных).
- Тип SQL-команды.
- Объекты БД:
  - функция;
  - поля;
  - таблица.

Аудит выявленных событий

Анализ события за любой период времени можно получить в виде графических и статистических отчетов по любым данным, даже тем, которые на первый взгляд не относятся к инциденту.

Аналитические возможности решения позволяют:

- строить профили работы всех пользователей;
- выявлять статистические аномалии в работе пользователей;
- составлять схемы распространения информации.

Подробные графические отчеты представлены в виде понятного и легкого в управлении веб-интерфейса, оптимизированного под работу на любых устройствах с выходом в Интернет, вне зависимости от операционной системы.

Просмотр «сырых» данных

Высокоэффективное хранение всего трафика объемом до 100 Тб и быстрый критериальный и полнотекстовый поиск информации позволяют анализировать данные за любой период времени вне зависимости от того, учтены они в политиках или нет. Данные хранятся в обезличенном виде благодаря технологии маскирования.

Выявление и расследование инцидентов / продолжение

Совместная работа трёх подсистем

- Мониторинг и выявление инцидентов.
- Хранилище больших данных.
- Мощная аналитическая система.

Мощная аналитическая система

Вся информация о несанкционированном доступе к базам данных за требуемый период времени доступна в разделе аналитики. Восстановить полную информационную картину возможно, даже если не были созданы соответствующие политики безопасности.

В едином центре управления доступно формирование политик информационной безопасности, проведение расследований, управление архивом данных.

Высокопроизводительная система хранения и поиска

Система класса DWH (Data Warehouse — хранилище данных) собственной разработки МФИ Софт обеспечивает индексацию и быстрый поиск по всем поступающим данным.

Система обеспечивает не только хранение данных, связанных с инцидентами безопасности, но и запись трафика всех баз данных и веб-приложений компании, без потери своих функциональных характеристик.

Мониторинг и выявление инцидентов

Система в автоматическом режиме проводит анализ информации в базах для предотвращения нарушений политик безопасности, определения аномалий и построения отчётности. Для выявления инцидента достаточно нескольких секунд.

Преимущества системы защиты баз данных «Гарда БД»

Высокая производительность: анализ десятков Тб за секунды

Масштабируемость

Интуитивно понятный интерфейс

Хранение всех ответов и запросов пользователей и приложений с возможностью ретроспективного анализа за любой период времени

Интеграция с SIEM и Ldap

Отсутствие стороннего лицензирования

Полноценная работа с трёхзвенной архитектурой взаимодействия с базами данных

Минимальное влияние на производительность сети и серверов СУБД

Реализация требований регуляторов

- 152-ФЗ «О персональных данных» от 21.07.2014
- 161-ФЗ «О национальной платежной системе» от 29.12.2014
- П-1119
- 382-П
- PCI DSS
- SOX
- HIPPA
- PDPA

Пилотный проект

МФИ Софт предоставляет вам возможность проверить работу решения на практике. Закажите пилотный проект, и мы бесплатно внедрим систему защиты баз данных «Гарда БД» в вашей компании для тестирования.

Внедрение «под ключ»

МФИ Софт осуществляет комплексную поддержку клиента на всех этапах сотрудничества — от выбора оптимальной конфигурации до инсталляции продукта, обучения персонала и технической поддержки:

- разработка технического решения, инсталляция комплекса;
- настройка и адаптация системы под индивидуальные потребности бизнеса;
- консультационная поддержка при работе с продуктом;
- техническая поддержка;
- послегарантийное обслуживание.

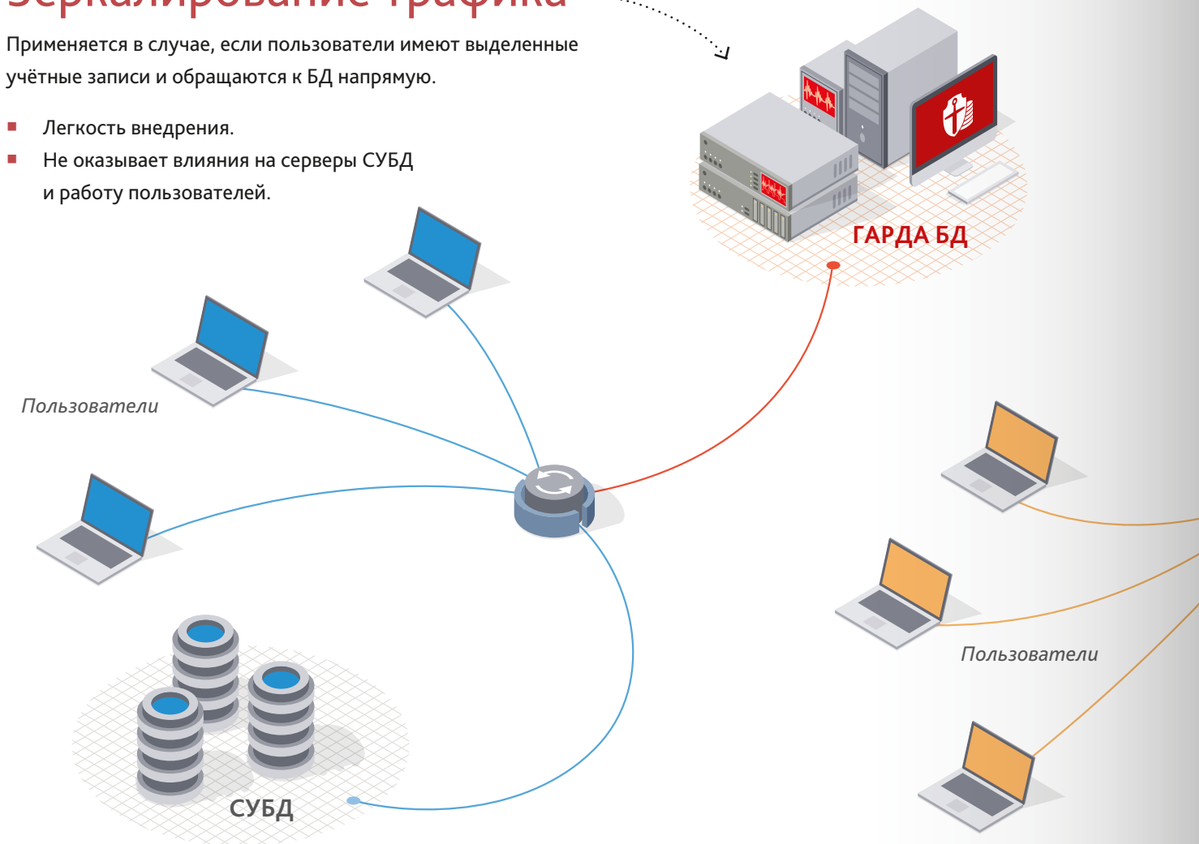
Схема внедрения

Гибкая архитектура решения позволяет быстро внедрить систему в любой компании, независимо от территориальной распределенности.

Зеркалирование трафика

Применяется в случае, если пользователи имеют выделенные учётные записи и обращаются к БД напрямую.

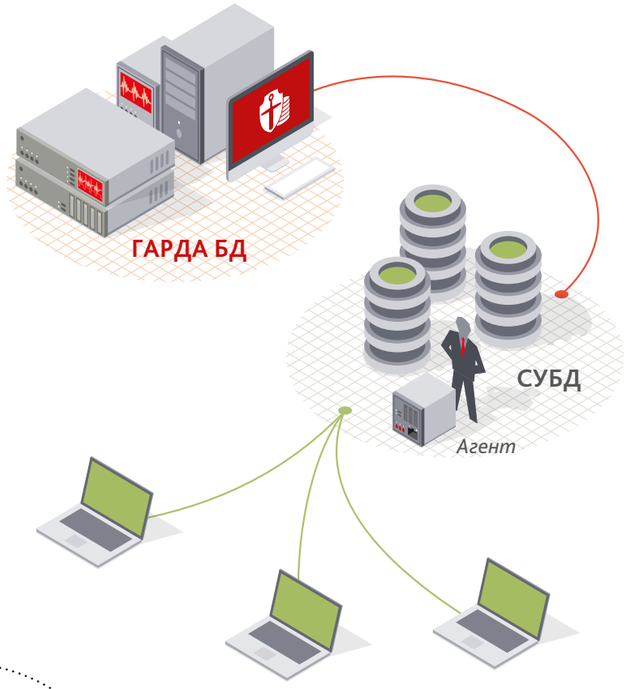
- Легкость внедрения.
- Не оказывает влияния на серверы СУБД и работу пользователей.



Агенты

Решение позволяет контролировать локальные и сетевые подключения к базам данных.

- Эффективный контроль привилегированных пользователей и администраторов.
- Нет необходимости приобретать дополнительное сетевое оборудование.



Активная защита. Сетевой экран

Решение позволяет блокировать нежелательные действия пользователей баз данных по различным параметрам, в соответствии с политиками безопасности.

- Интеллектуальная система самообучения модуля анализирует деятельность операторов БД для предотвращения ложных срабатываний.
- Повышенная отказоустойчивость системы обеспечена bypass-адаптером, который перенаправит трафик в обход сетевого экрана при его выключении.

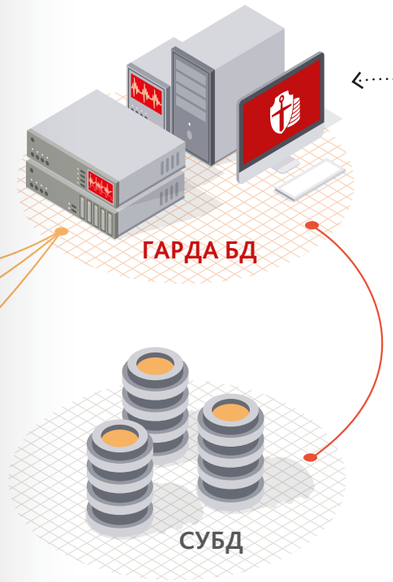


Схема внедрения / продолжение

Контроль веб-приложений

Возможность контролировать как SQL-серверы, так и веб-клиенты.

Виртуализация

Возможно внедрение решения как в физической, так и в виртуальной среде.

Решения МФИ Софт

СОРМ

Полный спектр систем СОРМ:
СОРМ 1 / СОРМ 2 / СОРМ 3

Гарда Предприятие

DLP-система нового поколения. Основные задачи, решаемые системой: контроль информационных потоков на предприятии, исполнение политики информационной безопасности, хранение архива бизнес-коммуникаций.

Гарда Монитор

Выявление и расследование сетевых инцидентов.

Периметр

Группа решений для предупреждения, обнаружения и подавления DDoS-атак в сетях передачи данных.

FMS Retail

Аппаратно-программный комплекс, предназначенный для выявления мошенничества в сети розничных продаж оператора сотовой связи.

FHS-01

Решение для оперативного выявления фактов bypass, on-net и off-net фрода при терминации трафика в сети оператора связи.

МФИ СОФТ

Свяжитесь с нами, чтобы посмотреть систему «Гарда БД» в действии!

Москва
Комсомольский проспект, д. 19А
8 (495) 540 88 10

Нижний Новгород
ул. Нартова, 6/6
8 (831) 422 11 61

ib.sales@mfisoft.ru
mfisoft.ru

ГАРДА БД

Информационная безопасность:
Аудит сетевого доступа
к базам данных и веб-приложениям