ГАРДА
ТЕХНОЛОГИИ

ВЫЯВЛЕНИЕ ВНУТРЕННИХ МОШЕННИКОВ И РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ПРИ ОБРАЩЕНИЯХ К БАНКОВСКИМ СУБД

Добрушский Сергей
Директор по разработке
20 февраля 2019

О РАЗРАБОТЧИКЕ

ГАРДА ТЕХНОЛОГИИ — РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компания обладает многолетним опытом в сфере информационных технологий и разрабатывает решения для различных задач безопасности.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Решения Гарды Технологии внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.

100 +
Внедрений на территории России

150 +
Высококвалифицированных сотрудников

10 лет
Опыт разработки систем высокой сложности

5
запатентованных технологий собственного исследовательского центра

ПОЛНОСТЬЮ РОССИЙСКИЕ РЕШЕНИЯ

- Собственная технологическая платформа для хранения информации не требует сторонних лицензий.
- Решения сертифицированы ФСТЭК.
- Включены в реестр отечественного программного обеспечения.

ОТ КОГО НУЖНО ЗАЩИЩАТЬСЯ?

БАЗЫ ДАННЫХ — ОСНОВНОЙ ИСТОЧНИК НАИБОЛЕЕ ЦЕННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИИ.

КРОМЕ ВЛАДЕЛЬЦЕВ ДАННЫХ ЭТА ИНФОРМАЦИЯ ИНТЕРЕСУЕТ МНОЖЕСТВО ДРУГИХ ЛЮДЕЙ.

ИНСАЙДЕРЫ

Хищения информации сотрудниками с целью продажи конкурентам или использования на новом месте работы.

ХАКЕРЫ

Целенаправленные атаки на базы данных для получения доступа к ним.

ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ

Контроль действий администраторов баз данных.

ХАЛАТНОСТЬ

Случайные утечки данных, совершенные по неосторожности.

ШТАТНЫЕ СРЕДСТВА КОНТРОЛЯ?

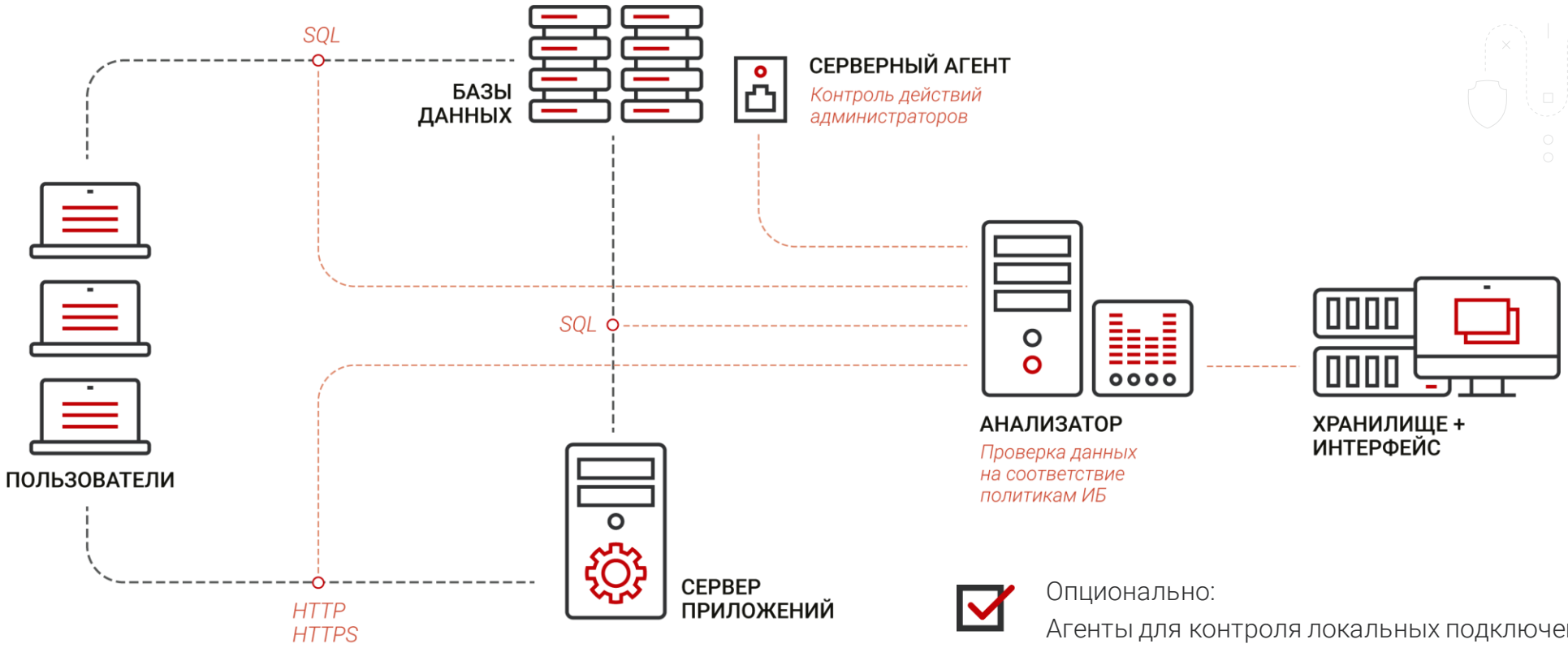
ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

ИСПОЛЬЗОВАНИЕ ШТАТНЫХ СРЕДСТВ АУДИТА БАЗ ДАННЫХ ВЛЕЧЕТ ЗА СОБОЙ ДОПОЛНИТЕЛЬНЫЕ ЗАТРАТЫ, И ПРИ ЭТОМ НЕ ДАЁТ НЕОБХОДИМОЙ ПОЛНОТЫ КОНТРОЛЯ.

- Требуют постоянного ручного контроля и специфических знаний пользователя.
- Существенно снижают производительность СУБД (10-40%).
- Отсутствие контроля привилегированных пользователей.
- Нет идентификации пользователя в трёхзвенной архитектуре.
- Отсутствие механизмов реагирования при нарушении.

СХЕМА ИНТЕГРАЦИИ DAM СИСТЕМЫ В СЕТЬ

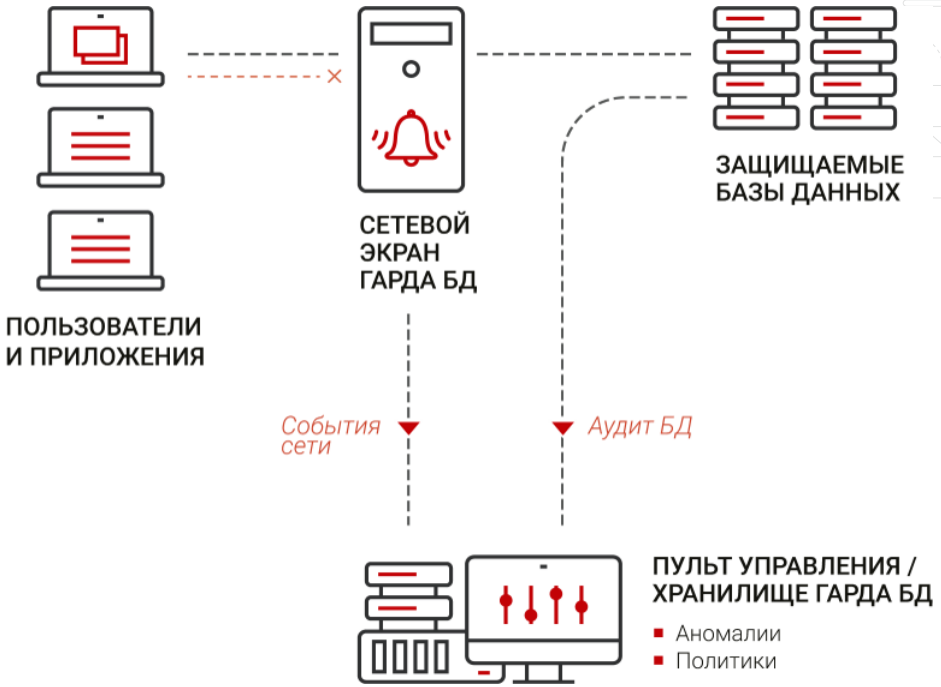


Опционально:
Агенты для контроля локальных подключений

DBF: АКТИВНАЯ ЗАЩИТА СУБД

РЕШЕНИЕ БЛОКИРУЕТ НЕЖЕЛАТЕЛЬНЫЕ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ, ПРОТИВОРЕЧАЩИЕ ПОЛИТИКАМ БЕЗОПАСНОСТИ.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА САМООБУЧЕНИЯ АНАЛИЗИРУЕТ ДЕЯТЕЛЬНОСТЬ ОПЕРАТОРОВ БД ДЛЯ ПРЕДОТВРАЩЕНИЯ ЛОЖНЫХ СРАБАТЫВАНИЙ.



Блокировка реализуется по принципу L3 Reverse Proxy Firewall, благодаря чему обеспечивается повышенная отказоустойчивость.

ТЕХНИЧЕСКИЕ ВОЗМОЖНОСТИ

ПОДДЕРЖИВАЕМЫЕ СУБД

- Oracle
- Microsoft SQL
- PostgreSQL
- MySQL
- Sun MySQL
- Teradata
- Firebird
- Sybase ASE
- IBM Netezza
- IBM DB2
- Линтер
- Apache Cassandra
- Interbase
- Hive *

*Как инструмент доступа к данным Hadoop

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ

- Хранение всех ответов и запросов пользователей и приложений с возможностью ретроспективного анализа за любой период времени.
- Маскирование платёжных данных в хранилище

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ (UBA)

- Автоматическое построение профилей деятельности сотрудников;
- Выявление отклонений и аномалий в работе.

КОНТРОЛЬ ВЕБ-ПРИЛОЖЕНИЙ

- Детальный разбор http/https-трафика с выделением данных из веб-форм;
- Контроль любых веб-приложений:
  - По протоколам передачи данных http/https;
  - По протоколам аутентификации Kerberos, NTLM;
  - Самописная аутентификация (web form authentification).

РЕШАЕМЫЕ ЗАДАЧИ + КЕЙСЫ

- Обнаружение активных СУБД
- Сканирование СУБД (классификация - уязвимости)
- Ретроспективный анализ (расследование инцидентов)
- Поведенческая аналитика для выявления угроз (скомпрометированные УЗ, аномальная активность, и.т.д.)

ГАРДА ТЕХНОЛОГИИ

ГАРДА БД

СПАСИБО ЗА ВНИМАНИЕ!

г. Нижний Новгород, ул. Нартова 6, корп.6

8 (831) 422 12 21

г. Москва, БЦ «Симонов Плаза»

+7 (495) 116-56-61

gardatech.ru