DATABASE MONITOR

АУДИТ БАЗ ДАННЫХ

На сегодняшний день большинство действий сотрудников так или иначе заключаются во взаимодействии с базами данных. При этом действия сотрудников в самой базе данных зачастую никак не контролируются. Для осуществления такого контроля предназначен продукт **Серчинформ Database Monitor**, который позволяет обеспечить мониторинг всех SQL-запросов и ответов на них. Использование данного продукта значительно повышает безопасность критических данных, а также предоставляет контроль доступа к конфиденциальным и чувствительным данным.

Database Monitor может работать как самостоятельный продукт, так и в интеграции с DLP-системой «КИБ Серчинформ». Совместное использование позволяет контролировать действия сотрудников как в инфраструктуре в целом, так и внутри рабочих БД, осуществляя таким образом бесшовное покрытие рабочего информационного пространства системами ИБ.

Database Monitor обладает широким функционалом в отношении баз данных MS SQL Server и PostgreSQL:

- Выявление выгрузки критичных данных из БД;
- Детектирование попыток нерегламентированного доступа к конфиденциальной информации;
- Аудит изменений в БД (удаление/добавление/изменение данных);
- Фиксация выполнения потенциально опасных действий с БД (выполнение вредоносных скриптов, SQL injection).

Database Monitor сохраняет **теневую копию запросов** к базе данных и ответов и производит глубокую контентную аналитику содержания, выявляя работу с критичными для бизнеса данными – персональные, финансовые, конфиденциальные и т.д. Например – запрос сотрудником спецификации стандартного заказа ключевого клиента с ценами покажется подозрительным, если это выходит за рамки его должностной роли. Или полная выгрузка клиентской базы – вряд ли существует бизнес процесс, при котором это действие является регламентированным для типового сотрудника. Для выявления таких фактов и применяется Database Monitor.

Серчинформ Database Monitor осуществляет **аудит запросов на изменение** к БД в онлайн-режиме 24/7. В рамки данного аудита попадает добавление/удаление/изменение данных. Данный аудит позволяет легко выявить, кто явился инициатором удаления из БД контактных данных ключевых клиентов, или кто изменил основные позиции ранее согласованной спецификации.

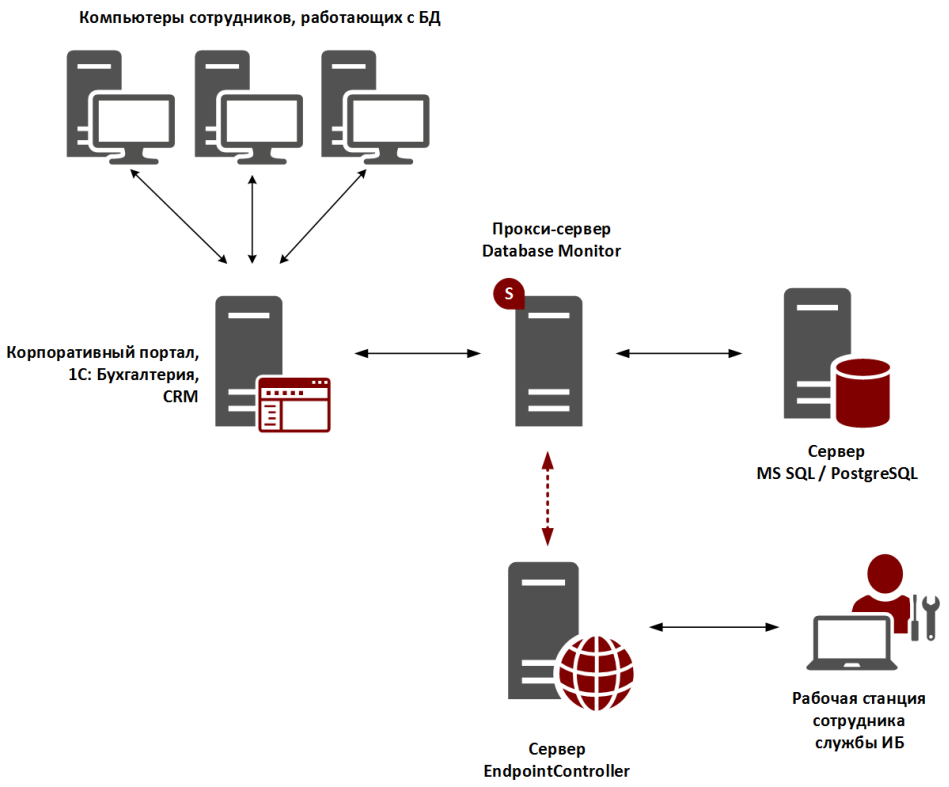
Одна из важных функций Database Monitor – это **полнотекстовый контентный анализ данных**. Таким образом программа способна выявить попытки получить или присвоить хранящуюся в базе данных информацию, представляющую коммерческую и другую тайну, а также прочую чувствительную информацию, тем самым детектируя факт подозрительной выгрузки из БД.

Аналитические возможности

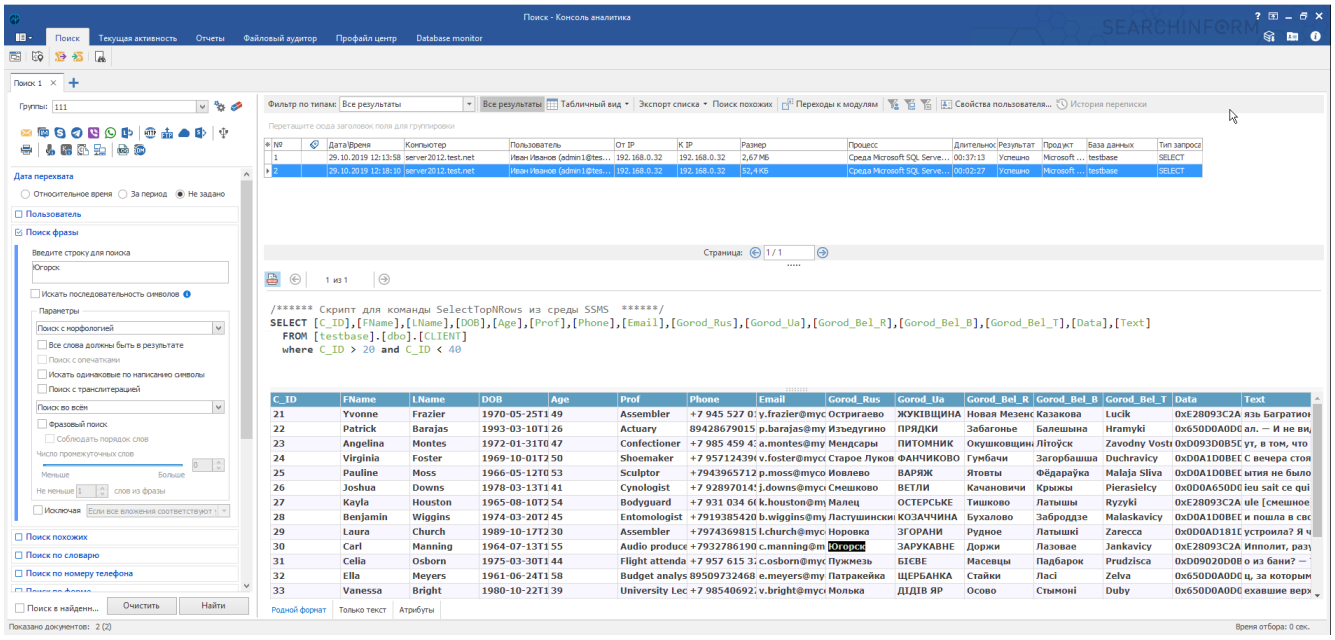
Поиск. Поиск по всем запросам к базе данных и ответам от нее. Возможно проведение поиска с учетом периода времени, пользователя, IP-адреса и других атрибутов. Можно искать фразы или текст на предмет точного или частичного совпадения, регулярные выражения и т.д. К примеру, можно найти все события удаления данных из базы, включая информацию о том, когда именно и кто их инициировал. Database Monitor позволяет осуществлять целевой поиск по всему массиву накопленных данных.

Визуализация. Аналитические возможности Аудита БД заключаются в осуществлении сбора статистики по действиям с базами данных и их визуализации при помощи гибко настраиваемых виджетов. Возможно представление данных за выбранный период в разрезе количества запросов, типов операций, пользователей, успешных и неудачных запросов и других атрибутов.

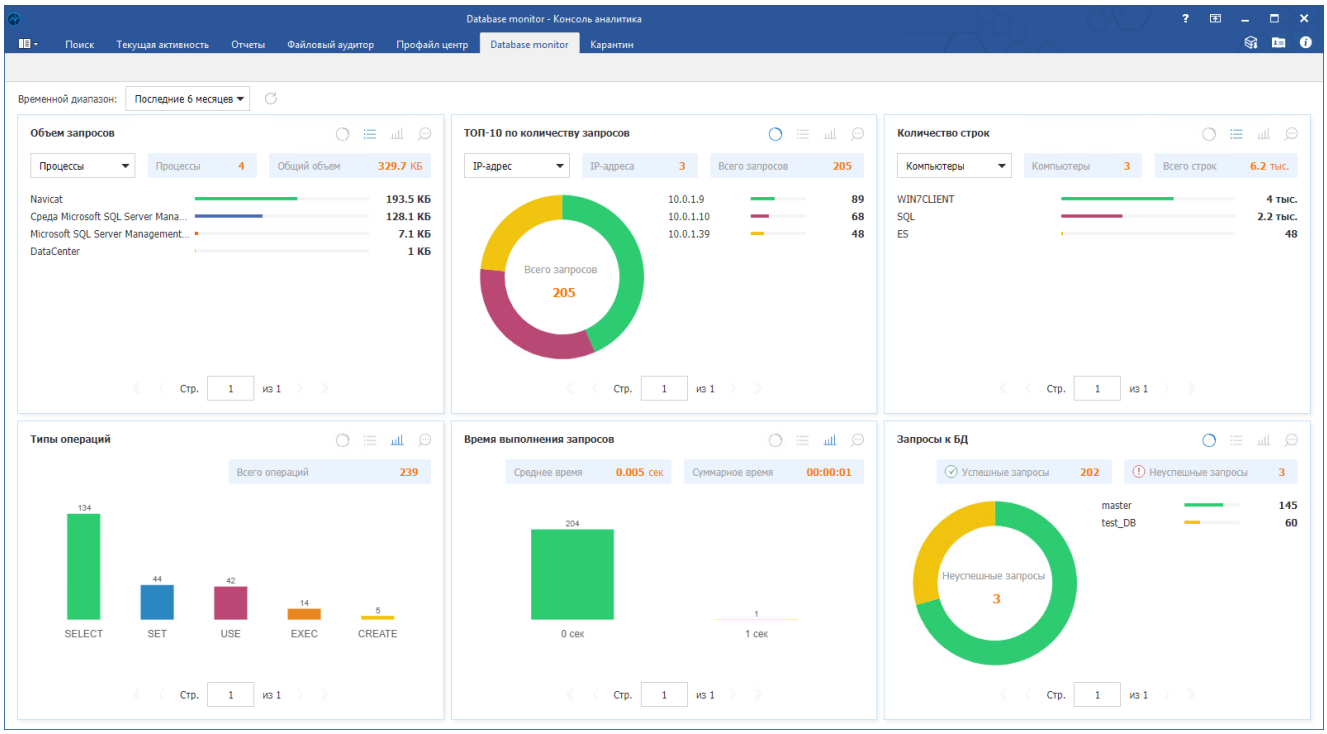
ПРИНЦИП РАБОТЫ



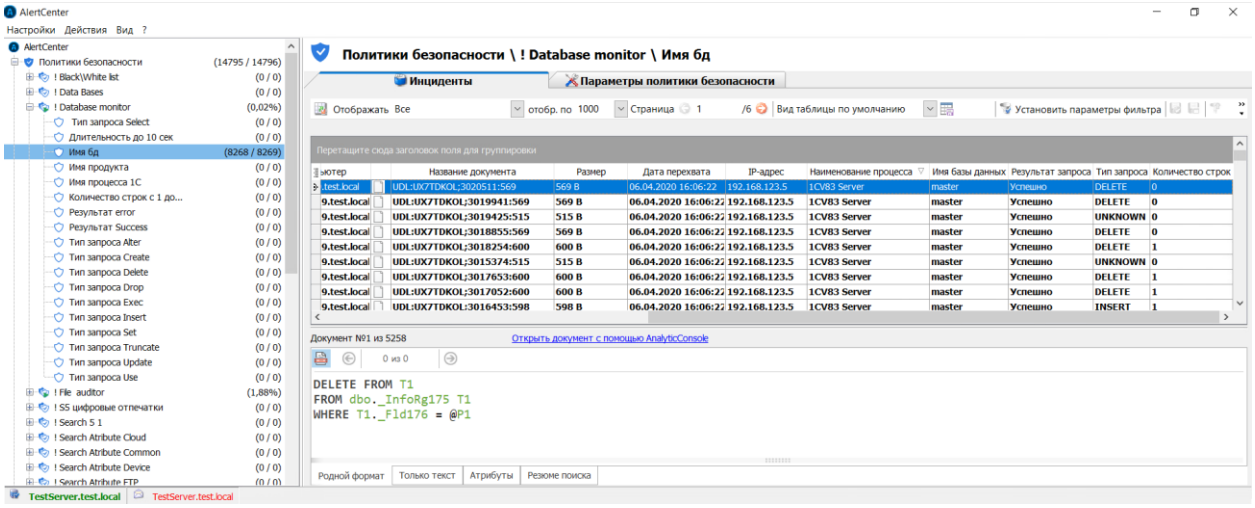
- На компьютер, который будет выполнять функции SQL прокси-сервера, устанавливается служба SearchInform Database Monitor.
- В настройках прокси-сервера задается номер порта, на который перенаправляются SQL-запросы.
- Запросы пользователей и ответы SQL-сервера проходят через прокси-сервер и записываются во временное хранилище, которое затем индексируются Search Server'ом.
- Поиск и отображение информации по перехваченным запросам к БД осуществляется в клиентском приложении AnalyticConsole.
- Компонент AlertCenter опрашивает подключенные базы данных Database Monitor по списку настроенных политик безопасности и оповещает сотрудника службы безопасности об инцидентах.



Представление поиска



Представление аналитических виджетов



Представление инцидентов

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ

	SQL прокси-сервер
Процессор	4-ядерный частотой 2 ГГц (64 бит)
Оперативная память	8 ГБ
Винчестер	250 ГБ (системный раздел диска – не менее 50 ГБ)
Сетевая карта	1 Гбит/с
Поддерживаемые операционные системы	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2
Файловая система	NTFS