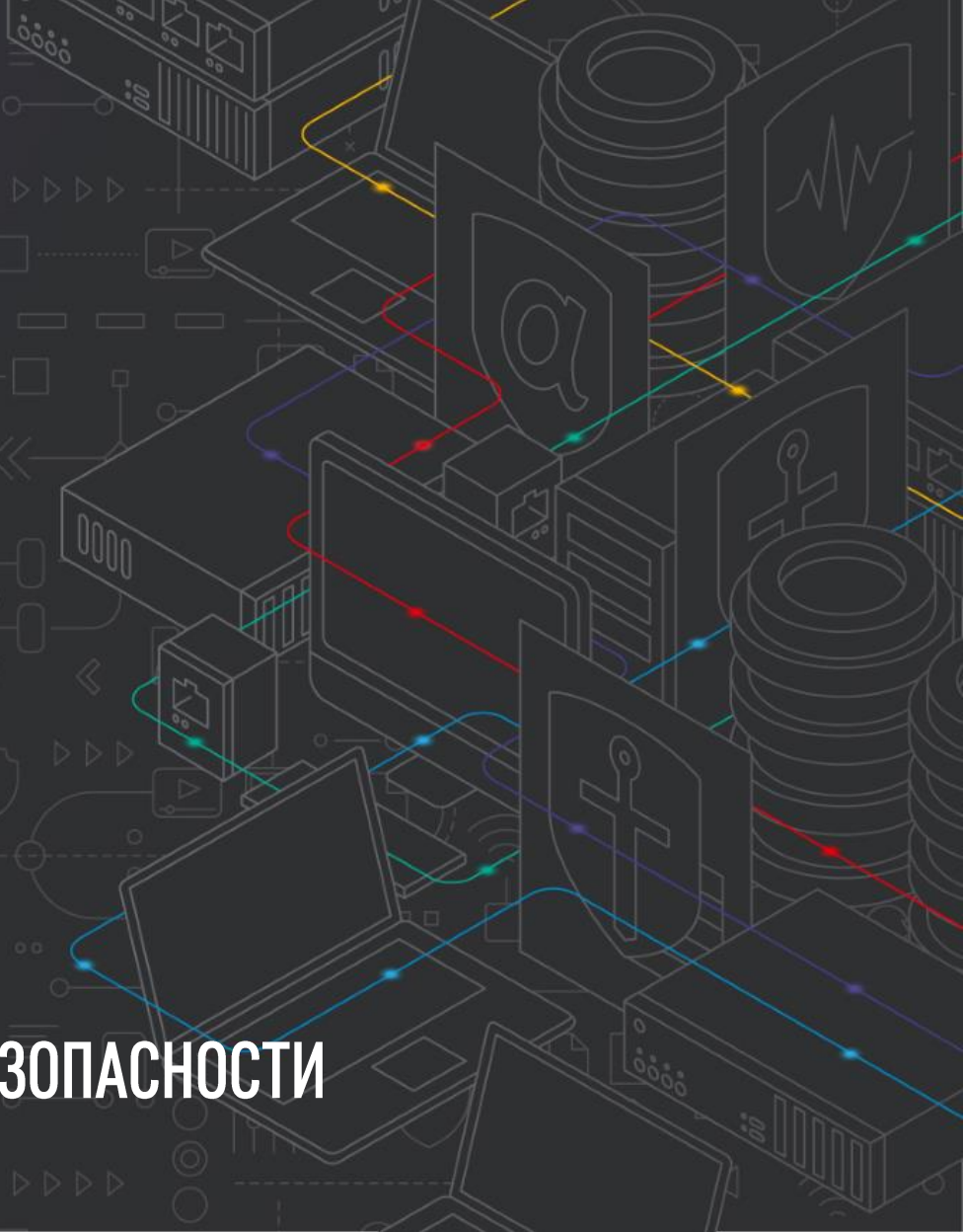
ГАРДА
ТЕХНОЛОГИИ

ГАРДА ТЕХНОЛОГИИ

РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ



О РАЗРАБОТЧИКЕ

ГАРДА ТЕХНОЛОГИИ

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 «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.

100+

Внедрений на территории России

180+

Высококвалифицированных сотрудников

12 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.

КАК МЫ РАБОТАЕМ

ГАРДА ТЕХНОЛОГИИ

РАЗРАБОТКА

Разработка и внедрение под задачи клиента

- Оперативная разработка специализированных решений под задачи клиента
- Инсталляция на месте с учётом модификаций и особенностей сети
- Выбор оптимальной конфигурации решения

ТЕСТИРОВАНИЕ

Предварительное тестирование, высокая скорость внедрения

- Широкие возможности предварительного тестирования продуктов
- Минимальный срок поставки
- Удаленное изменение параметров лицензии

ПОДДЕРЖКА

Высокий уровень службы поддержки

- Единая система обработки запросов в системе Help deck
- 2 линия технической поддержки — специалист выполняет задачи по администрированию
- 3 линия технической поддержки — специалист выполняет сложные настройки, вносит при необходимости изменения в работу компонентов ИС
- Все специалисты имеют образования в сфере информационной безопасности
- Высокий уровень SLA

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

DLP-СИСТЕМА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

СИСТЕМА ДЛЯ ЗАЩИТЫ ОТ УТЕЧЕК ИНФОРМАЦИИ И ВЫЯВЛЕНИЯ ПОТЕНЦИАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НОВЫЙ ВЗГЛЯД НА DLP

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

Обычно настройка, сопровождение
и анализ результатов работы DLP-системы
занимает слишком много времени.

«ГАРДА ПРЕДПРИЯТИЕ» РАЗРАБОТАНА ДЛЯ РЕАЛИЗАЦИИ ЕЖЕДНЕВНЫХ ЗАДАЧ ИБ-СПЕЦИАЛИСТОВ — УПРОЩАЕТ И АВТОМАТИЗИРУЕТ РУТИННУЮ РАБОТУ

Гарда Предприятие выявляет нарушения и угрозы сразу после запуска, до завершения всех этапов внедрения и настройки DLP.

Выявление существенных рисков, категоризация информации, быстрое создание политик ИБ и их проверка - все интуитивно понятно даже без чтения инструкции.

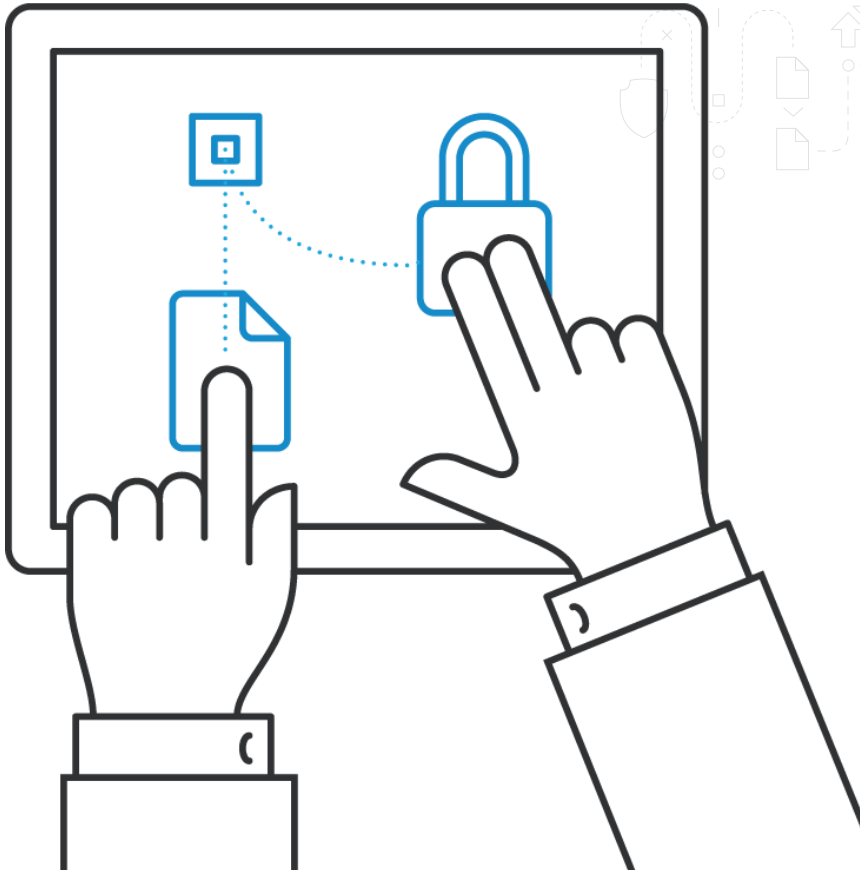
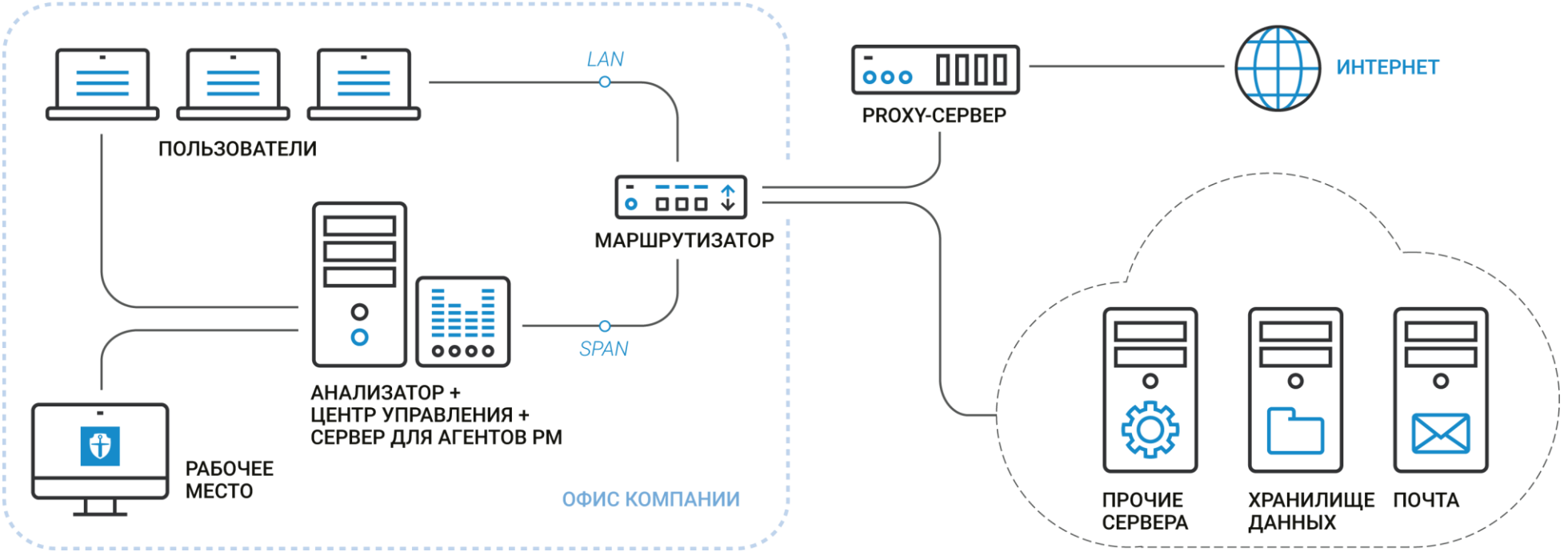


СХЕМА ВНЕДРЕНИЯ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

Вся функциональность системы, включая управление агентами рабочих мест, работу с https, перехват и анализ трафика, хранение данных, поставляется на 1U/2U или 4U сервере, в зависимости от количества рабочих мест и требуемого периода хранения.

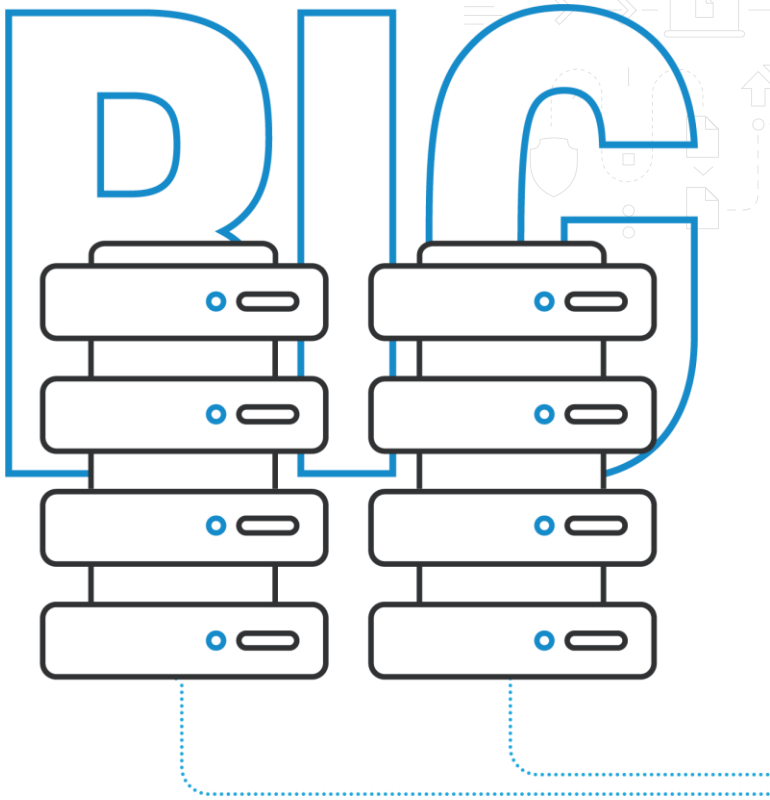


ХРАНЕНИЕ ДАННЫХ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ПРЕДПРИЯТИЕ — ОДНА ИЗ ПЕРВЫХ DLP-СИСТЕМ, СПРОЕКТИРОВАННЫХ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ BIG DATA



Подсистема хранения — эксклюзивная разработка Гарда Технологии, созданная для решения актуальных проблем обычных DLP-систем и обеспечивает:

BIG DATA

- Хранение широкого спектра данных, обрабатываемых в компании – сведения об инцидентах, маркеры информационных потоков, факты совершения коммуникаций между объектами наблюдения и т.д.
- Высокую скорость доступа к данным – их анализ, и быстрый поиск;
- Низкую стоимость хранения по сравнению со схожими решениями.

Данные поступают в комплекс из различных источников (сетевой трафик, почтовые серверы, рабочие места и др.) и хранятся в собственной базе для дальнейшего анализа.

КОНТРОЛЬ РАБОЧИХ МЕСТ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ПОДДЕРЖКА ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ УСТАНОВКИ АГЕНТА ГПР

WINDOWS

- Windows XP SP3
- Windows 7
- Windows 8
- Windows 10
- Windows Server 2008, 2012

LINUX

- Astra Linux Special Edition версии 1.6 и выше
- Astra Linux Common Edition версии 1.9 и выше
- Ubuntu версии 16 и выше

MAC OS

Версии 10.13 и выше

КОНТРОЛЬ РАБОЧИХ МЕСТ

ОБЕСПЕЧЬТЕ КОМПЛЕКСНЫЙ МОНИТОРИНГ КОМПЬЮТЕРОВ «ГАРДА ПРЕДПРИЯТИЕ» НЕ ТОЛЬКО АНАЛИЗИРУЕТ КОММУНИКАЦИИ И ИНФОРМАЦИЮ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММ И ПЕРИФЕРИИ, НО И ДАЁТ ШИРОКИЕ ВОЗМОЖНОСТИ ПО КОНТРОЛЮ РАБОЧИХ МЕСТ

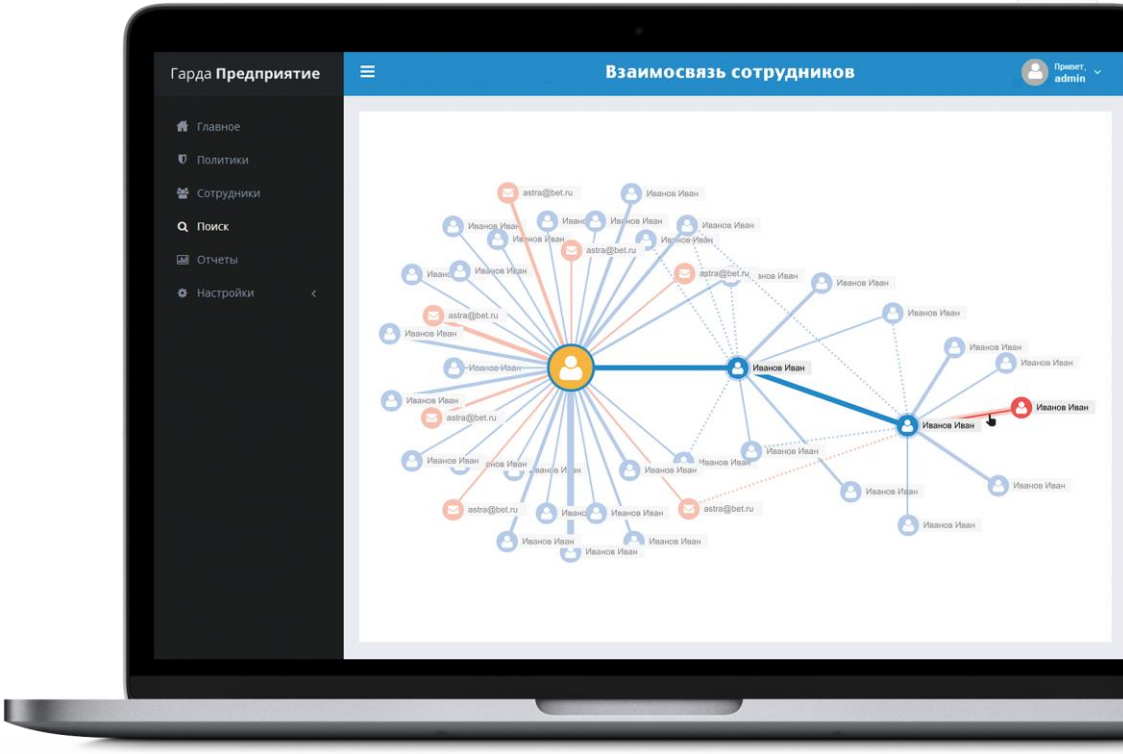
- Теневое копирование данных, передаваемых на внешние устройства
- Контроль печати
- Снимки экрана рабочего стола по расписанию или условию
- Просмотр и запись экрана рабочего стола в реальном времени
- Контроль Skype, Telegram, Viber
- Контроль HTTPS (соцсети, веб-почта и др. сайты и сервисы)
- Контроль приложений и журналирование активности
- Блокировка использования приложений
- Блокировка подключаемых устройств (белые списки)
- Блокировка передачи конфиденциальных данных
- Сканирование рабочих мест для обнаружения конфиденциальных данных
- Перехват облачных хранилищ

ВЗАИМОСВЯЗИ СОТРУДНИКОВ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ИНТЕРАКТИВНЫЙ ОТЧЁТ НАГЛЯДНО ДЕМОНСТРИРУЕТ ОБЛАКО КОММУНИКАЦИЙ СОТРУДНИКА КАК ВНУТРИ КОМПАНИИ, ТАК И СВЯЗИ С ВНЕШНЕЙ СРЕДОЙ, ОТРАЖАЕТ ИНТЕНСИВНОСТЬ КОММУНИКАЦИЙ И СРЕДСТВА ПЕРЕДАЧИ ИНФОРМАЦИИ



КАРТОЧКА СОТРУДНИКОВ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ЭКОНОМЬТЕ ВРЕМЯ НА РУТИННЫХ ЗАДАЧАХ. ГАРДА ПРЕДПРИЯТИЕ АВТОМАТИЧЕСКИ ЗАПОЛНЯЕТ ПРОФИЛИ СОТРУДНИКОВ.

ВЫБЕРИТЕ ИНТЕРЕСУЮЩЕГО СОТРУДНИКА
И УВИДИТЕ ЕГО «ЛИЧНОЕ ДЕЛО»:

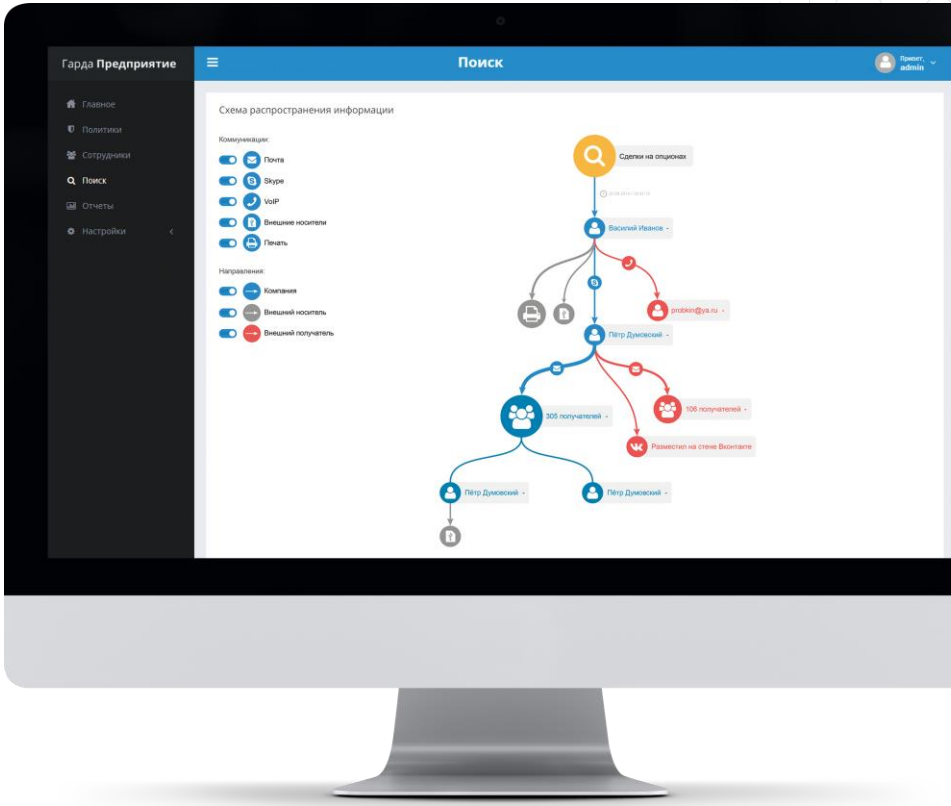
- Идентификационные данные – должность, фото и др.
- Статистика по деятельности
- Учётные записи различных сервисов
- Последние события

КОНТЕНТНЫЕ МАРШРУТЫ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

НАГЛЯДНО ПРЕДСТАВЛЯЕТ МАРШРУТ ДВИЖЕНИЯ ЛЮБОЙ ИНФОРМАЦИИ ОТ ПЕРВОЙ КОММУНИКАЦИИ ДО МОМЕНТА ПЕРЕДАЧИ ЗА ПРЕДЕЛЫ ОРГАНИЗАЦИИ. В МАРШРУТЕ УЧИТЫВАЮТСЯ КАК ПОЛЬЗОВАТЕЛИ, ТАК И КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ



Отчёт позволяет оперативно расследовать инцидент, выявить сговоры и найти несанкционированных обладателей информации до того, как конфиденциальные данные покинут компанию.

ТЕХНОЛОГИИ АНАЛИЗА

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

В СИСТЕМЕ «ГАРДА ПРЕДПРИЯТИЕ» РЕАЛИЗОВАНЫ НАИБОЛЕЕ ЭФФЕКТИВНЫЕ ТЕХНОЛОГИИ АНАЛИЗА:

ПОИСК ПОХОЖИХ

Позволяет найти документы и фрагменты документов в пересылаемой пользователями информации. Выявляет нелегитимный доступ и распространение информации.

ЛИНГВИСТИЧЕСКИЙ АНАЛИЗ

Алгоритмы лингвистического анализа позволяют просто и эффективно находить нужную информацию при помощи встроенного поиска. Также алгоритмы повышают эффективность срабатывания политик безопасности.

ШАБЛОНЫ (REGEXP)

Технология обнаружения структурированных данных в потоке информации (номера паспортов, кредитных карт, адреса электронной почты и др.). Позволяет защищать персональные данные, финансовую документацию.

ОПТИЧЕСКОЕ РАСПОЗНАВАНИЕ ТЕКСТА НА ИЗОБРАЖЕНИЯХ (OCR)

Система поддерживает распознавание текста на изображениях для дальнейшего анализа. Технология OCR не требует дополнительного лицензирования.

ПРЕИМУЩЕСТВА DLP-СИСТЕМЫ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

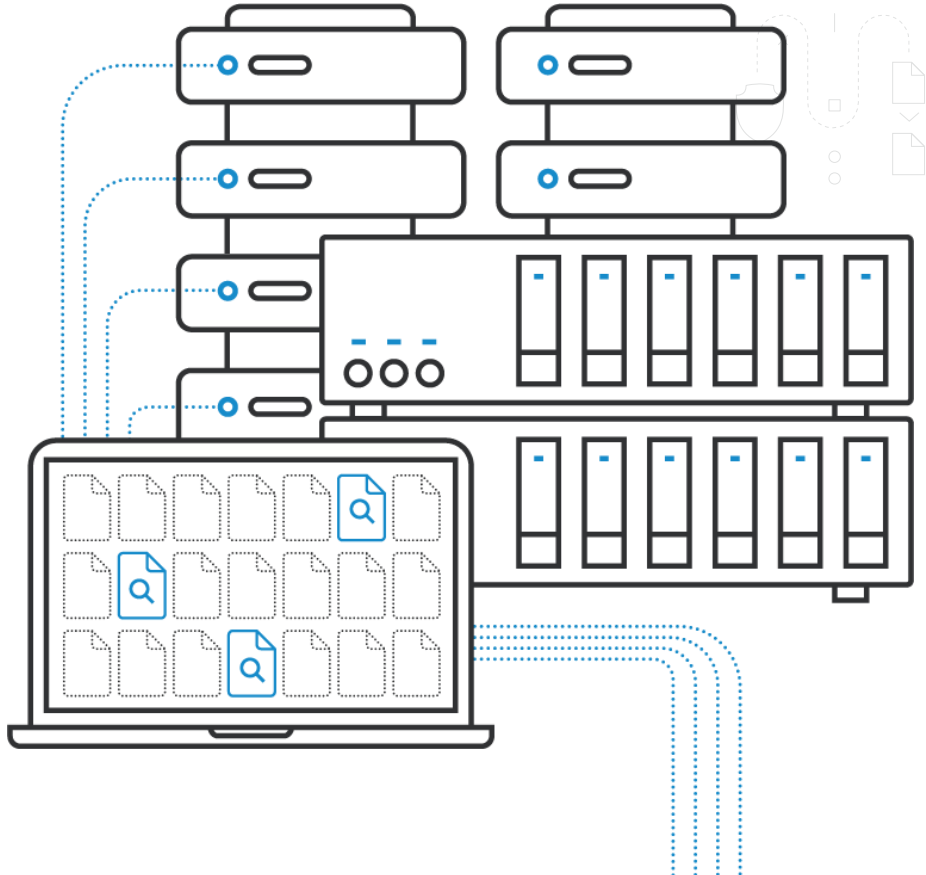
- Высокая скорость работы (no SQL)
- Модули неразрывны друг с другом и поставляются на единой аппаратной платформе (весь функционал)
- Все программные компоненты являются разработкой компании «Гарда Технологии» и не требуют дополнительного лицензирования (нет дополнительных затрат)
- Кроссплатформенность — управление доступно с любого устройства и операционной системы
- Агенты под Windows, Linux, Mac
- Интерфейс системы разработан в режиме одного окна, прост и понятен любому пользователю, построен по принципу от общего к частному.

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ПРЕИМУЩЕСТВА DLP-СИСТЕМЫ

- Начинает работать сразу после внедрения, до формирования политик безопасности компании
- Высокая скорость поиска данных и формирования отчетов
- Высокоэффективная система хранения данных, оптимальна для больших объемов и регионально распределенных компаний
- Интуитивно понятный интерфейс, использование интерактивных отчетов



ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

ГАРДА БД

АУДИТ И ЗАЩИТА БАЗ ДАННЫХ И ВЕБ-ПРИЛОЖЕНИЙ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

ГАРДА БД
ГАРДА ТЕХНОЛОГИИ

«ГАРДА БД» ОБЕСПЕЧИВАЕТ БЕЗОПАСНОСТЬ СУБД И НЕЗАВИСИМЫЙ АУДИТ ОПЕРАЦИЙ С БАЗАМИ ДАННЫХ И БИЗНЕС-ПРИЛОЖЕНИЯМИ

Защита от утечек информации, хранящейся в БД

Аудит всех операций с БД в режиме реального времени

Контроль действий привилегированных пользователей

Контроль удаленного доступа сотрудников

Выявление и предотвращение попыток внешнего вторжения в СУБД

Блокирование нежелательных запросов к БД и веб-приложениям

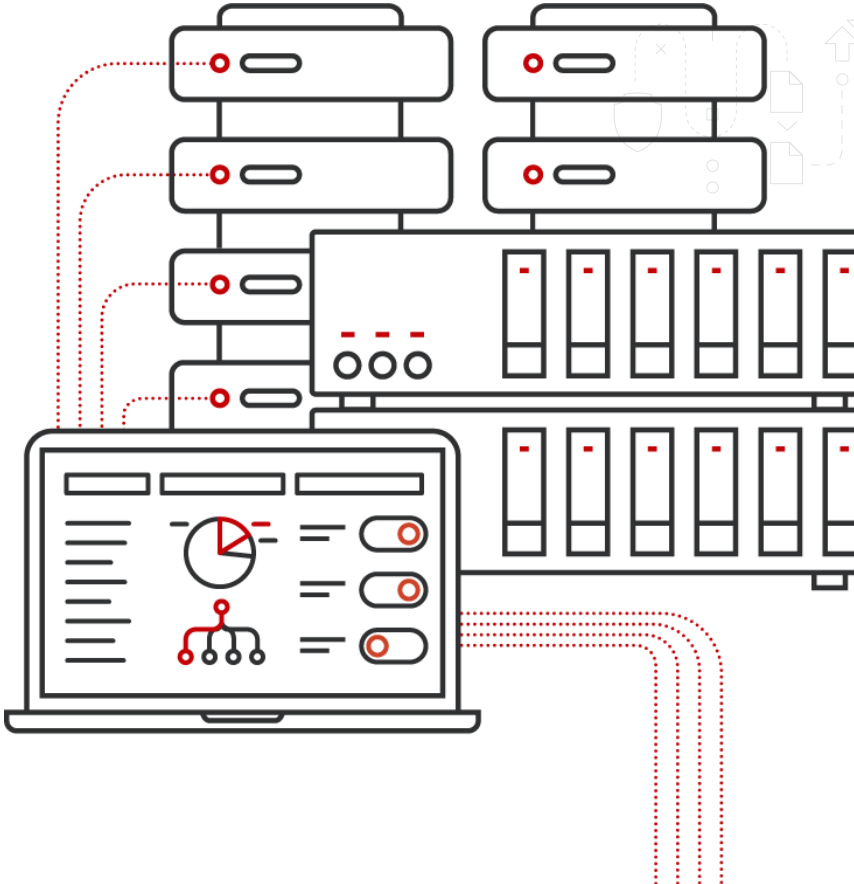
Обнаружение всех БД в компании, их классификация и сканирование на уязвимости

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

- Предотвращение выгрузки и продажи критичных данных клиентов, в том числе персональных данных, данных кредитных карт и т.д.
- Контроль манипуляций с клиентскими базами, накрутки KPI менеджерами
- Проверка БД на обезличенность при их передаче, например при их клонировании для целей тестирования
- Разграничение доступа к СУБД для аттестации информационных систем
- Выявление не оптимально настроенных конфигураций СУБД с точки зрения стандартов и лучших практик по информационной безопасности
- Предотвращение мошенничества и прямых хищений денежных средств с использованием БД и бизнес-приложений компании
- Выявление несанкционированного разворачивания теневых, нелегитимных и неконтролируемых баз данных со стороны администраторов
- И другие



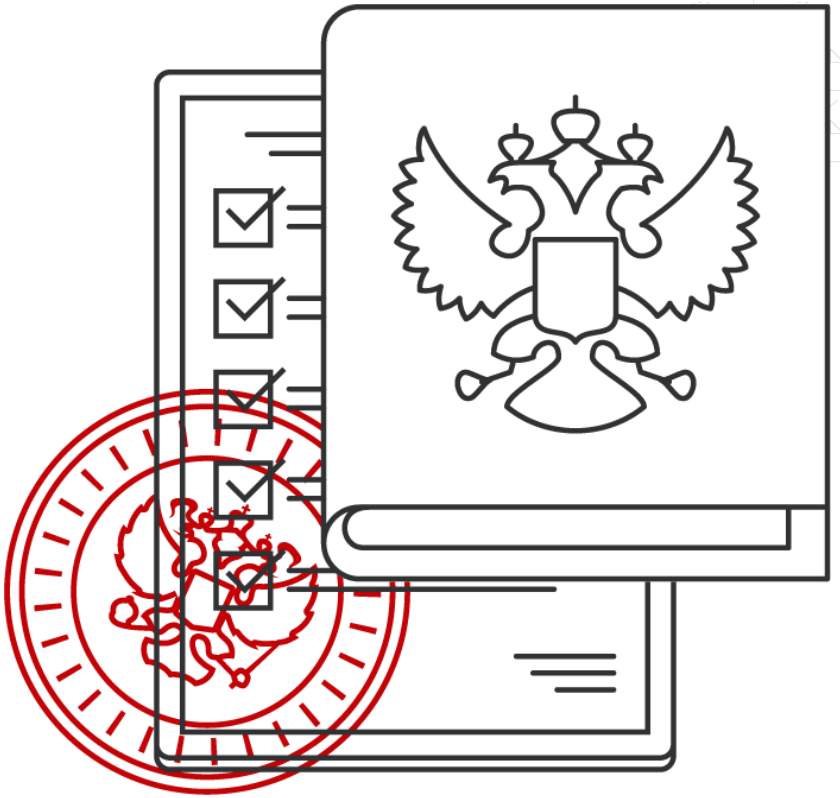
ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

СИСТЕМА ПОМОГАЕТ ВЫПОЛНИТЬ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

- **8-ФЗ.** Обеспечение доступа к информации государственных органов
- **152-ФЗ.** О персональных данных
- **187-ФЗ.** Безопасность объектов КИИ РФ
- **Приказ ФСТЭК №17.** Требования к защите информации в ГИС
- **Приказ ФСТЭК №21.** Обеспечение безопасности обработки ПДн
- **Приказ ФСТЭК №239.** Меры безопасности для значимых объектов КИИ
- **Приказ МинКомСвязи РФ №104.** Обеспечение безопасности для информационных систем общего пользования
- **ГОСТ Р 57580.1-2017.** Безопасность финансовых операций
- **СТО БР ИББС.** Стандарт по обеспечение ИБ банков РФ
- **GDPR.** Европейский регламент по защите ПДн
- **PCI DSS.** Международный стандарт безопасности данных платежных систем



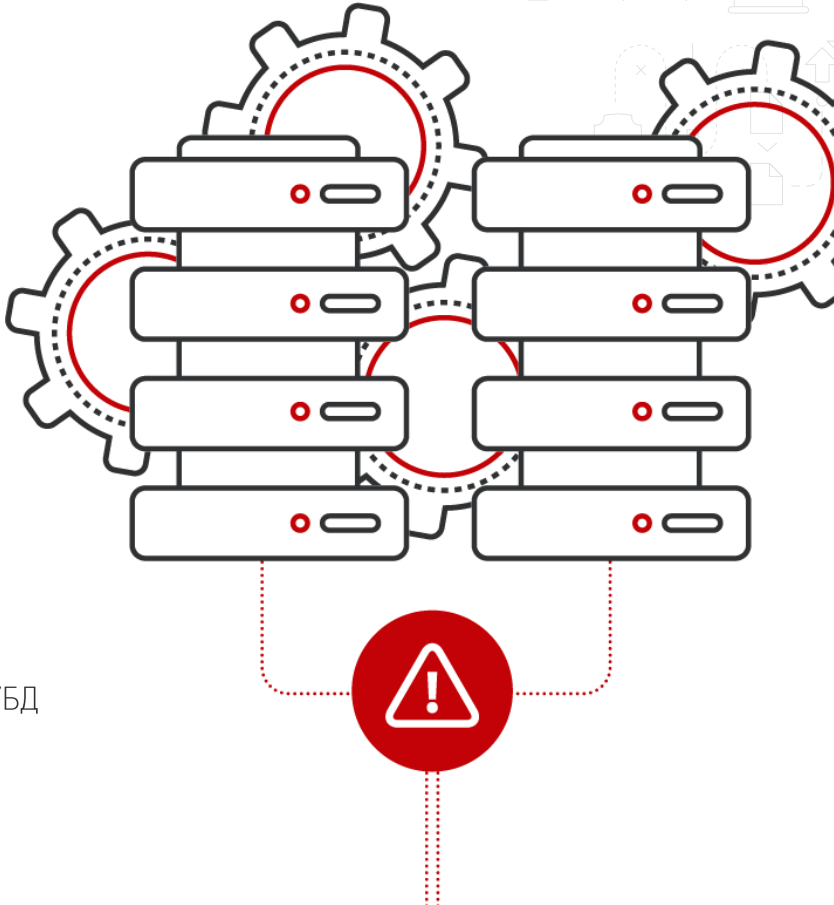
ПОМОГУТ ЛИ ШТАТНЫЕ СРЕДСТВА КОНТРОЛЯ?

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

ИСПОЛЬЗОВАНИЕ ШТАТНЫХ СРЕДСТВ АУДИТА БАЗ ДАННЫХ ВЛЕЧЁТ ЗА СОБОЙ ДОПОЛНИТЕЛЬНЫЕ ЗАТРАТЫ И НЕ ОБЕСПЕЧИВАЕТ ПОЛНОГО КОНТРОЛЯ

- Требуют постоянного ручного контроля и специфических знаний пользователя
- Существенно снижают производительность СУБД (10-40%)
- Отсутствие контроля привилегированных пользователей
- Невозможность блокировки действий пользователей
- Нет идентификации пользователя в трёхзвенной архитектуре
- Отсутствие механизмов реагирования при нарушении
- Невозможность расследования инцидента при нарушении работоспособности самой СУБД

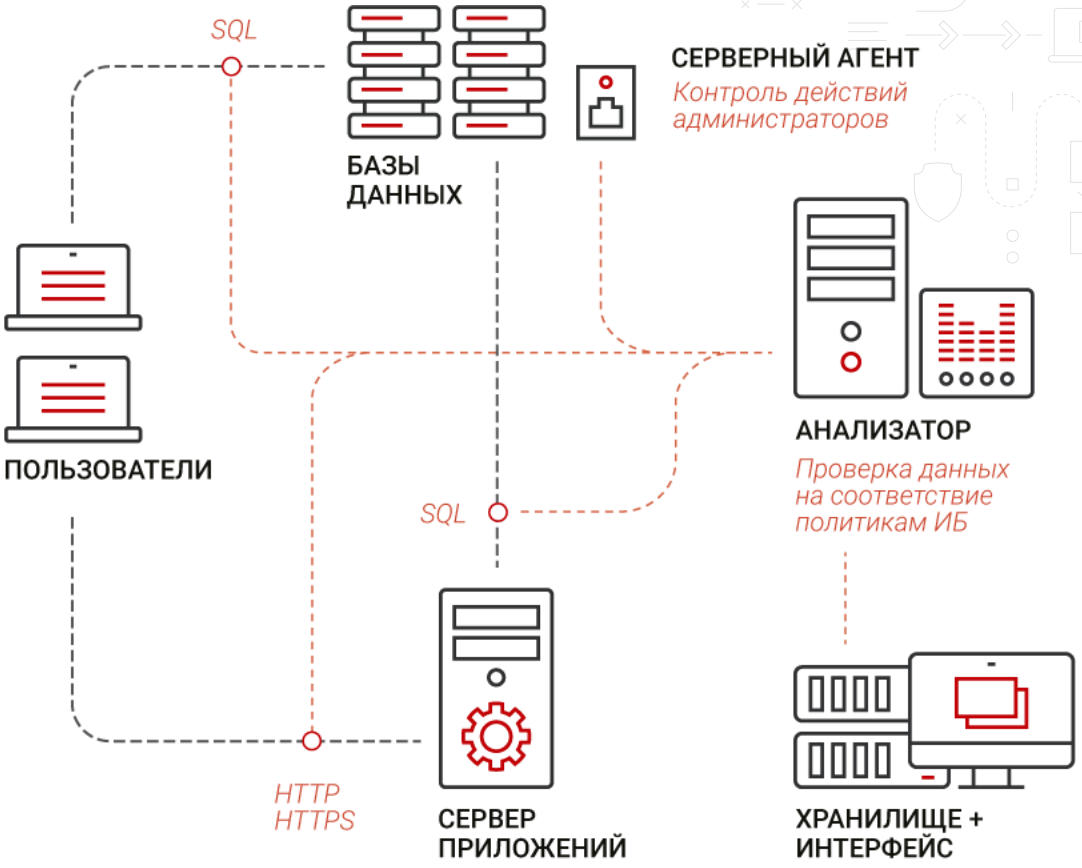


ЗЕРКАЛИРОВАНИЕ ТРАФИКА

ГАРДА БД
ГАРДА ТЕХНОЛОГИИ

ПРИМЕНЯЕТСЯ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ, КОТОРЫЕ ОБРАЩАЮТСЯ К БД НАПРЯМУЮ ИЛИ ЧЕРЕЗ ТРЕХЗВЕННЫЕ ПРИЛОЖЕНИЯ

Используются агенты для контроля локальных подключений либо перенаправления всего сетевого трафика к базам данных.



Горизонтальное масштабирование

Позволяет защищать высоконагруженные, в том числе территориально-распределенные системы любого масштаба из единого интерфейса

АКТИВНАЯ ЗАЩИТА || СЕТЕВОЙ ЭКРАН

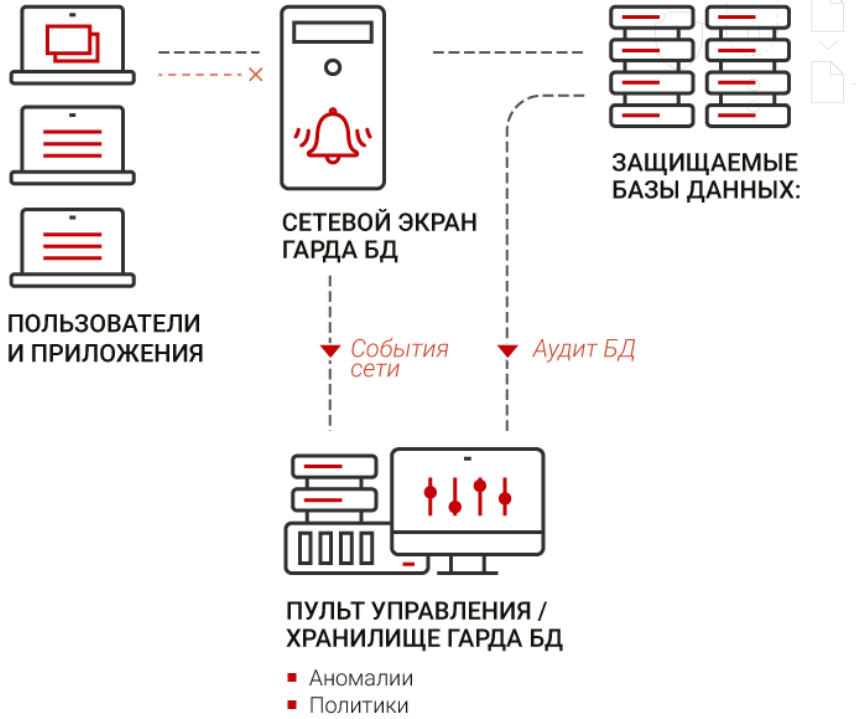
ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

БЛОКИРУЕТ НЕЖЕЛАТЕЛЬНЫЕ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ, ПРОТИВОРЕЧАЩИЕ ПОЛИТИКАМ БЕЗОПАСНОСТИ

Умная система самообучения анализирует деятельность операторов БД для предотвращения ложных срабатываний. Для гарантирования доступности защищаемых баз данных сетевой экран ставится в режиме отказоустойчивого кластера.

- ☑ Возможность дешифрации HTTPS-трафика по принципу Man In the middle (MITM)
- ☑ Возможность реализации **системы разграничения прав доступа** к СУБД для аттестации ИС, использующих несертифицированные СУБД



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

Гибкий конструктор политик и блокировки по правилам на агенте предотвращают утечку данных с уведомлениями о заблокированных сессиях в интерфейсе системы.

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

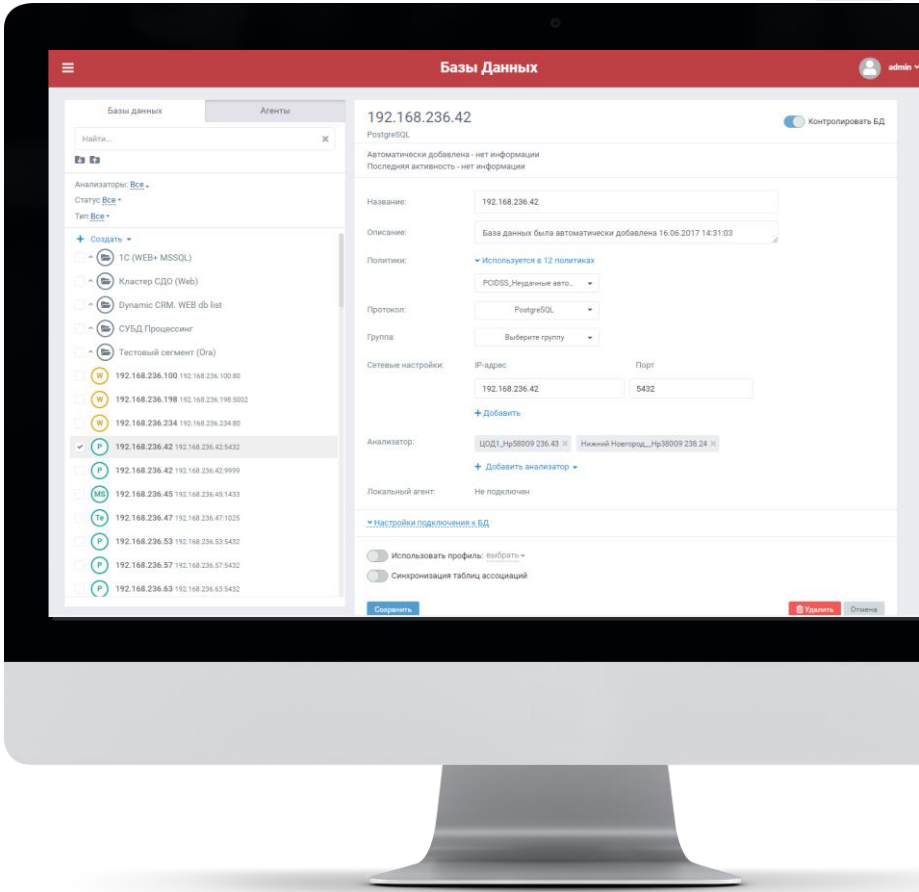
КРИТЕРИИ ФОРМИРОВАНИЯ ПОЛИТИК

- IP-адрес клиента
- Имя пользователя в БД
- Имя пользователя в ОС
- Название клиентского ПО
- Результат аутентификации
- Дата/время запроса
- Запрашиваемые/передаваемые поля таблицы, синонимы, представления
- Объём данных ответа/запроса
- Имя объекта БД
- Ключевое слово
- Тип SQL-команды
- Количество записей в ответе

ОБНАРУЖЕНИЕ И КЛАССИФИКАЦИЯ БД

СИСТЕМА АВТОМАТИЧЕСКИ НАХОДИТ НОВЫЕ БД, НЕ СТОЯЩИЕ НА КОНТРОЛЕ

- Всегда актуальный перечень СУБД компании.
- Обнаружение новых БД (создание новых ИС/АС).
- Выявление открытия новых портов, изменения IP-адресов СУБД



СКАНИРОВАНИЕ БАЗ ДАННЫХ

«ГАРДА БД» ПРОВОДИТ СКАНИРОВАНИЕ КОНТРОЛИРУЕМЫХ БАЗ ДАННЫХ. ЭТО ПОЗВОЛЯЕТ РЕШАТЬ ЗАДАЧИ, СВЯЗАННЫЕ НЕ ТОЛЬКО С КОНТРОЛЕМ ДОСТУПА, НО И С НЕКОРРЕКТНЫМИ НАСТРОЙКАМИ БЕЗОПАСНОСТИ.

КЛАССИФИКАЦИЯ

- Поиск местонахождения критичной информации
- Создание политик по результатам сканирования
- Настройка уровня угроз

УЯЗВИМОСТИ

- Неустановленные обновления
- Проверка оптимальности конфигурации СУБД
- База проверок на уязвимости

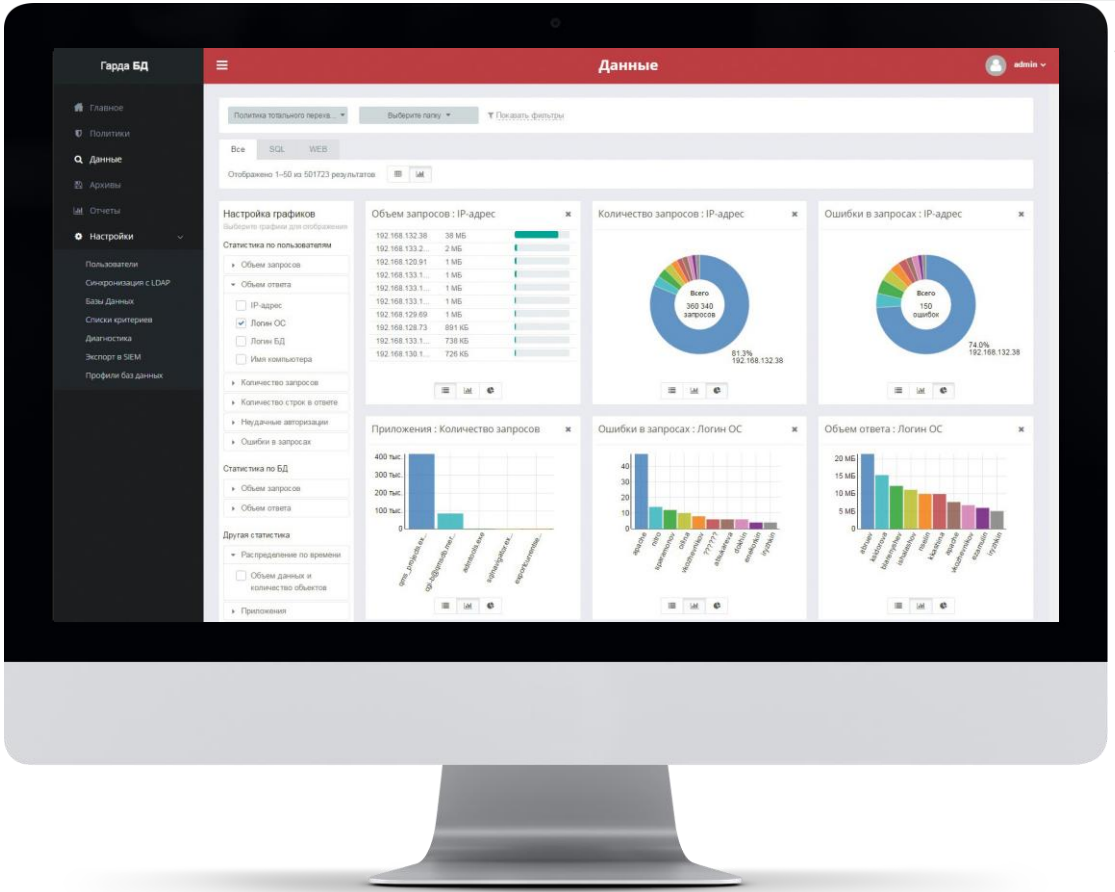
МАТРИЦЫ ДОСТУПА

- Построение карты доступа вида «Пользователь – Объект доступа (таблицы ,функции) – Типа прав доступа»
- Сравнение текущей картины с эталонной

КОНТРОЛЬ И АНАЛИТИКА

ВСТРОЕННЫЕ СРЕДСТВА АНАЛИТИКИ ПОЗВОЛЯЮТ ВЫЯВЛЯТЬ ОТКЛОНЕНИЯ В ОБЫЧНЫХ СЦЕНАРИЯХ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ БД И ПРЕДОСТАВЛЯЮТ НАГЛЯДНЫЕ СТАТИСТИЧЕСКИЕ ОТЧЕТЫ

- Интерактивная отчётность
- Конструктор отчётов с возможностью анализа любого объёма данных за любой промежуток времени
- Возможность создания индивидуального дашборда
- Поведенческий анализ пользователей БД (UEBA)
- Уведомление о нарушениях по электронной почте
- Уведомление о выявленных аномалиях в SIEM



ГАРДА БД: ЗАЩИТА «БОЛЬШИХ ДАННЫХ»

ГАРДА БД ГАРДА ТЕХНОЛОГИИ

ГАРДА БД ОБЕСПЕЧИВАЕТ ЗАЩИТУ BIG DATA: РЕЛЯЦИОННЫХ (ХРАНЯТСЯ В ТАБЛИЦАХ), НЕ РЕЛЯЦИОННЫХ (ХРАНЯТСЯ В СПЕЦИАЛЬНЫХ КЛАСТЕРНЫХ ХРАНИЛИЩАХ С ВОЗМОЖНОСТЬЮ РАСПРЕДЕЛЕННОЙ ОБРАБОТКИ).

Журнал данных. Возможность группировки данных по времени – логинам - приложениям и другим свойствам

Контролируем доступ к любым Big Data системам через Rest API

Полностью поддерживаем протокол HTTP до уровня данных

Поддержка Hortonworks Data Platform

Унифицируем подходы к защите реляционных и NoSQL баз данных

Защита BIG DATA

- Контроль доступа к Big Data системам через Rest API
- Поддержка протокола http/https
- Поддержка Hortonworks Data Platform
- Унификация подходов к защите реляционных и NoSQL баз данных
- Профиль учитывает особенности работы каждого сотрудника

Данные вашей компании являются BIG DATA, если они:

- Занимают большой объём >100 Тб
- Слабо структурированы
- Приходят из множества источников
- Должны обрабатываться в режиме реального времени
- Растут в размере хранения более чем на 50% в год

ДИНАМИЧЕСКОЕ ПРОФИЛИРОВАНИЕ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

Встроенные средства аналитики позволяют выявлять отклонения от обычных сценариев работы пользователей БД и формируют наглядные отчёты по инцидентам.

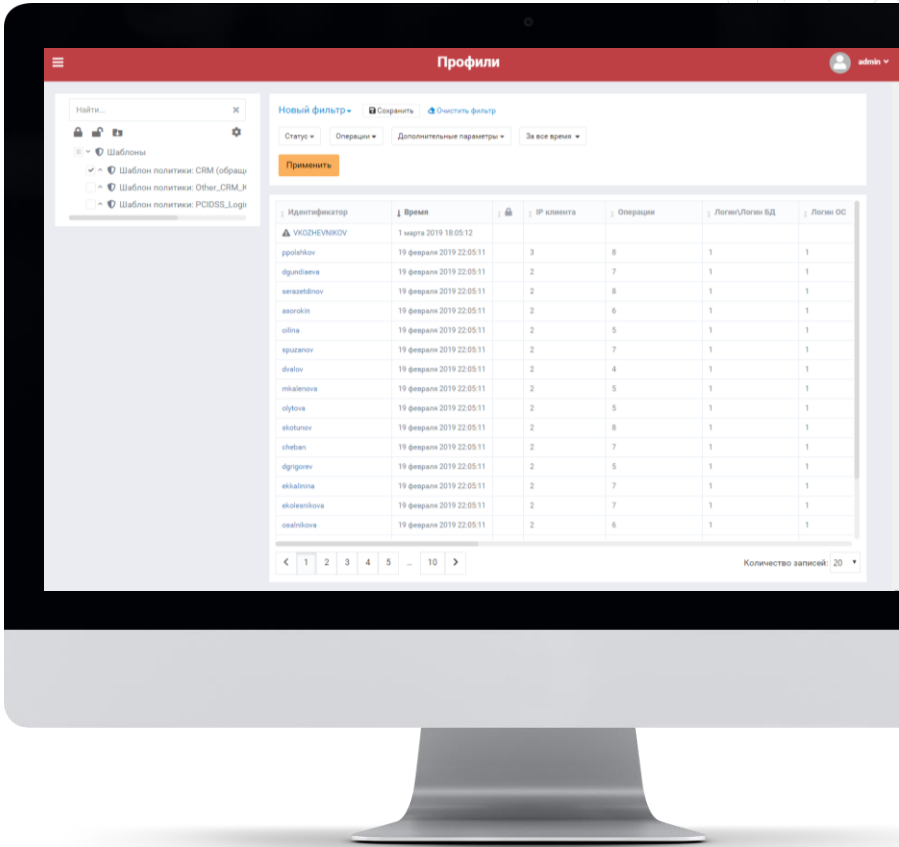
АВТОМАТИЧЕСКОЕ ПОСТРОЕНИЕ ПРОФИЛЕЙ В РЕЖИМЕ ОБУЧЕНИЯ

Учитываются:

- Логины, приложения, IP-адреса, названия таблиц и полей
- Особенности работы каждого сотрудника
- Информация о регионе

ВЫЯВЛЕНИЕ ОТКЛОНЕНИЙ ОТ ПРОФИЛЕЙ

- Нетипичное поведение для данного пользователя (чужие IP-адреса, ранее не используемые таблицы, приложения и рабочие места)
- Статистические аномалии:
  - Большое количество запросов
  - Большие выгрузки
  - Много неуспешных авторизаций



КОНТРОЛЬ ВЕБ-ПРИЛОЖЕНИЙ И 1С

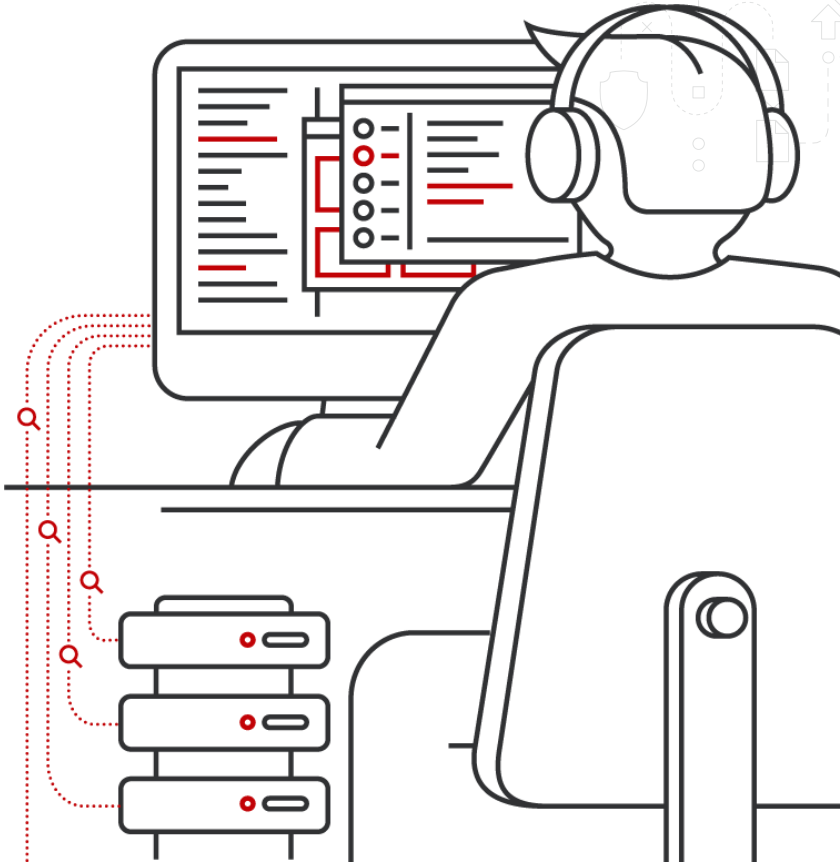
ГАРДА БД
ГАРДА ТЕХНОЛОГИИ

КОНТРОЛЬ ВЕБ-ПРИЛОЖЕНИЙ

- Детальный разбор HTTP/HTTPS-трафика с выделением данных из веб-форм
- Возможность дешифрации HTTPS-трафика как в пассивном, так и в режимах работы «вразрыв»
- Персонификация пользователей с возможностью выделения учетных записей
- По протоколам передачи данных HTTP/HTTPS
- По протоколам аутентификации Kerberos, NTLM
- Аутентификация (web form authentification)

МОНИТОРИНГ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМАХ 1С

Служба информационной безопасности в интерфейсе системы видит не только обращения к СУБД, но и все **пользовательские действия**, позволяющие понимать, какая информация, находящаяся в системе 1С, была модифицирована, а к какой были обращения со стороны пользователей, с привязкой к учётным записям.



ОСОБЕННОСТИ РЕШЕНИЯ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

Возможность ретроспективного анализа по сохраненным данным объёмом свыше 100 ТБ

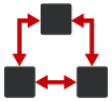
Аудит доступа к БД всех филиалов компании из единого центра

Интеграция со всеми популярными SIEM

Интерактивные отчеты и понятная аналитика на основе всех запросов и ответов БД, статистика инцидентов

Встроенная система выявления аномалий и поведенческого анализа действий пользователей

Возможность анализа трафика на скорости более 10 Гбит/с



Полноценная работа с трёхзвенной архитектурой взаимодействия с БД

Минимальное влияние на производительность сети и серверов СУБД

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

Отсутствие стороннего лицензирования

ПРЕИМУЩЕСТВА РЕШЕНИЯ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

- Более 30 поддерживаемых российских и зарубежных СУБД, в том числе на технологиях BigData
- Поддержка распределённой кластерной инсталляции и централизованного управления из единого интерфейса
- Множество способов подачи трафика (агенты, подача данных с TAP-устройств/SPAN, GRE, ERSPAN)
- Высокая производительность (обработка 10ГБит/с и выше), неограниченная возможность кластеризации
- Сетевой экран с функцией блокировки и динамической балансировки трафика
- Возможность дешифрации HTTPS-трафика как в пассивном режиме, так и при инсталляции «в разрыв»
- Персонификация пользователей с возможностью выделения учетных записей
- Гибко настраиваемые фильтры, автоматическое формирование списков критериев для использования в политиках

ПРЕИМУЩЕСТВА РЕШЕНИЯ

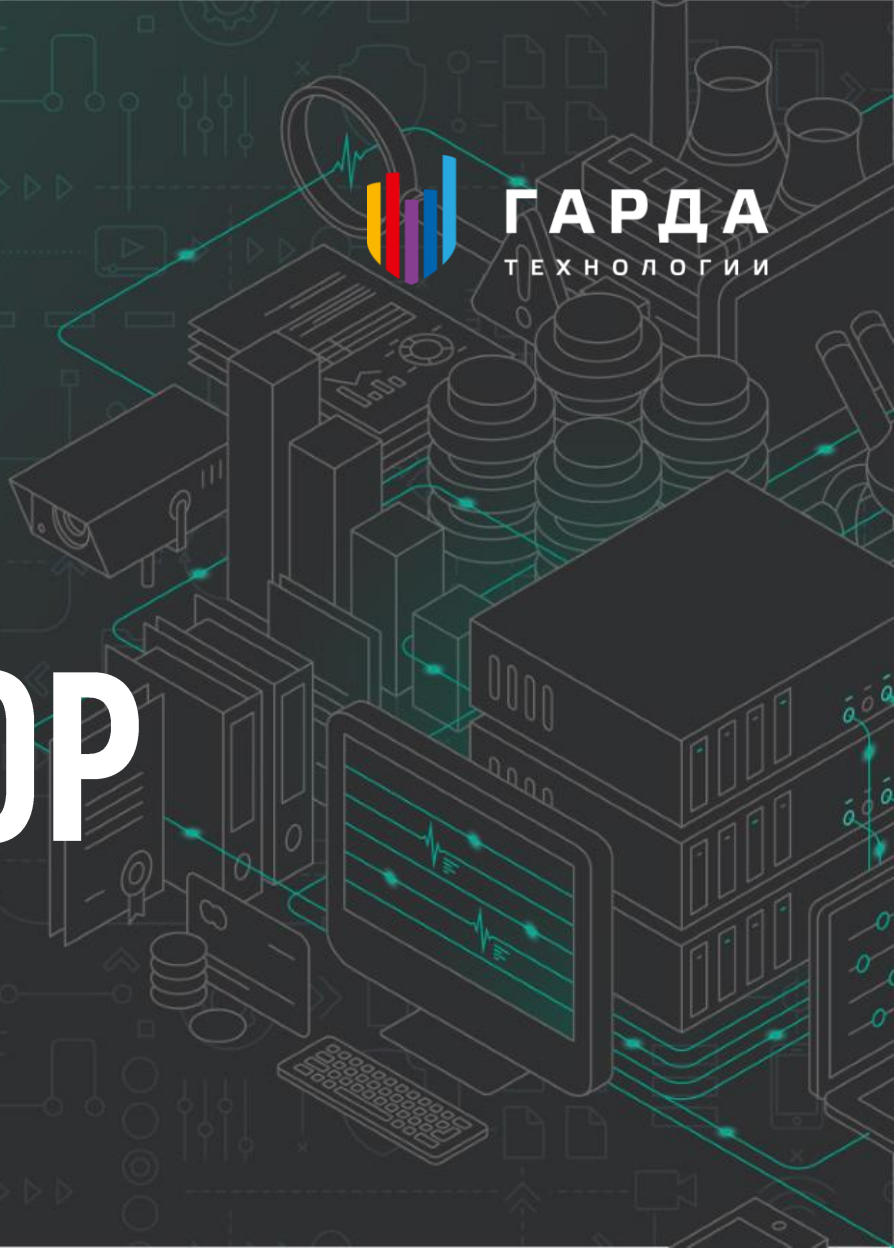
ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

- Сводные отчёты (в том числе отчёт по уязвимостям)
- Встроенный модуль контроля Web-приложений, не требующий отдельных лицензий
- Контроль неявных обращений к СУБД
- Динамическое профилирование (UEBA) с уведомлениями и отчётами
- Доменная авторизация
- Входит в реестр отечественного ПО
- Сертификат ФСТЭК
- Не зависит от того, каким образом достаются данные из базы или веб-приложения (ноут, телефон, прочее)
- Незаметность для пользователя (не надо ставить агентов на рабочие места) – важно для тех кто работает удаленно

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ



ГАРДА МОНИТОР

ВЫЯВЛЕНИЕ УГРОЗ И РАССЛЕДОВАНИЕ СЕТЕВЫХ ИНЦИДЕНТОВ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

«ГАРДА МОНИТОР» — СИСТЕМА ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ И РАССЛЕДОВАНИЯ СЕТЕВЫХ ИНЦИДЕНТОВ, АНАЛИЗА ТРАФИКА, ОБНАРУЖЕНИЯ АТАК НА ПЕРИМЕТРЕ И ВНУТРИ СЕТИ

Выявляет признаки вредоносного ПО в сетевом трафике

Обеспечивает **тотальную запись** сетевых потоков

Осуществляет мониторинг и сбор данных о сетевой активности

Анализирует события сетевой безопасности

Выявляет атаки на периметре и внутри сети

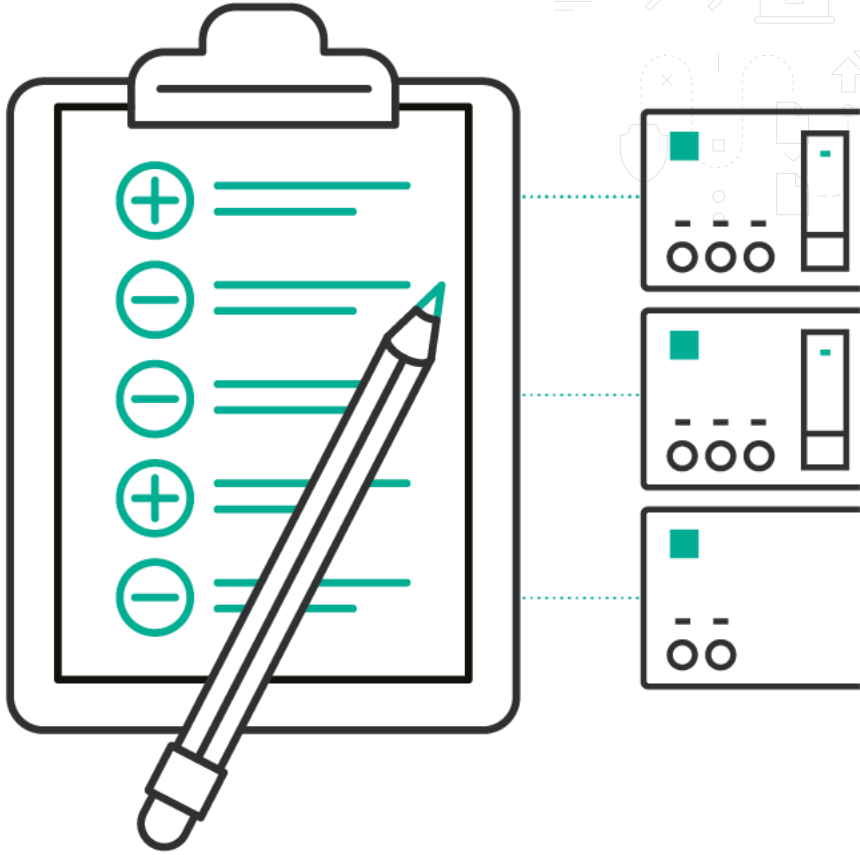
Позволяет выполнять **расследования** сетевых инцидентов

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

- Детектирование загрузки файлов с внешних неизвестных хостов
- Обнаружение попыток удаленного выполнения кода
- Выявление использования слабой парольной политики в компании
- Обнаружение использования протоколов анонимных сетей DarkNet (Tor, I2P)
- Контроль использования некорпоративного DNS
- Выявление использования программного обеспечения, предназначенного для загрузки пиратского контента (Torrent)
- Обнаружение сетевых протоколов на нестандартных портах
- Выявление майнинга
- И прочие



ПРИНЦИП РАБОТЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

КОНТРОЛЬ СЕТЕВЫХ КАНАЛОВ

- На соответствие передаваемых потоков данных политикам информационной безопасности
- На выявление аномальной активности

ОПТИМИЗИРОВАННОЕ ХРАНЕНИЕ

- Гибкие настройки параметров записи:
  - Запись с сохранением «сырых» данных
  - Запись только статистики по всем потокам
- Индексация и быстрый поиск по всему объёму поступающих данных благодаря высокопроизводительной системе хранения

ПЕРЕХВАТ, АНАЛИЗ И ЗАПИСЬ

IP-трафика в режиме реального времени

УДОБНЫЙ ВЕБ-ИНТЕРФЕЙС

Многоуровневые отчеты и настраиваемый рабочий экран для удобного управления и решения задач сетевой форензики

ИЗВЕСТНЫЕ ПРОБЛЕМЫ ПРИ АНАЛИЗЕ РАБОТЫ СЕТИ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

БОЛЬШОЕ КОЛИЧЕСТВО ПОТОКОВ

Анализ логов каждой системы занимает много времени и требует специальных знаний

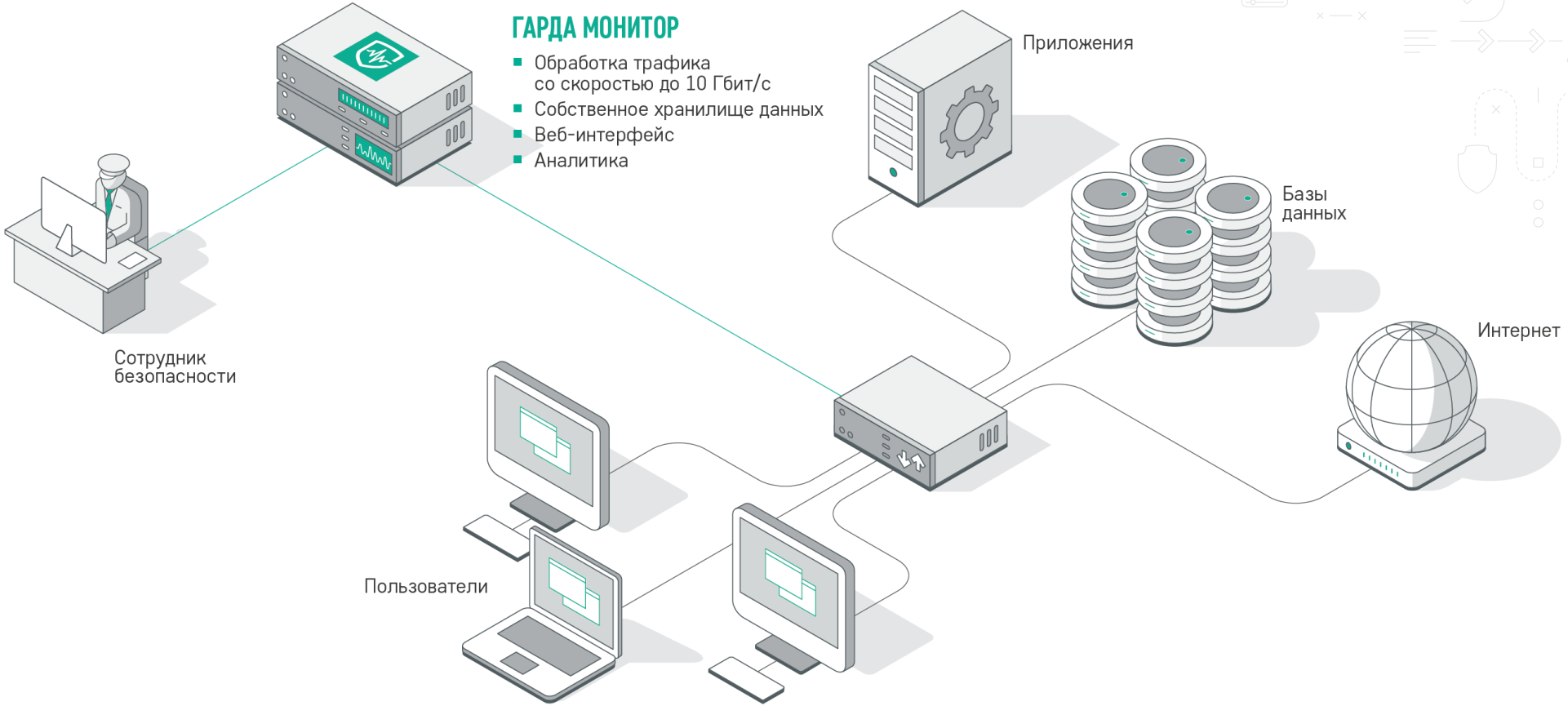
НЕЗАЩИЩЁННЫЕ ЛОГИ

Возможность изменения этих логов администратором системы

ПИК НАГРУЗКИ ПРИ АУДИТЕ

Аудит сетевой активности на системах и устройствах создаёт дополнительную нагрузку на них

СХЕМА


ГАРДА МОНИТОР
Обработка трафика со скоростью до 10 Гбит/с
Собственное хранилище данных
Веб-интерфейс
Аналитика
Приложения
Базы данных
Интернет
Сотрудник безопасности
Пользователи

КЕЙСЫ || 1

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

1 ВЫЯВЛЕНИЕ ДЕЙСТВИЙ ВРЕДОНОСНОГО ПО

- Аномально большое количество почтовых сообщений с компьютера (спам-бот)
- Аномально большое количество DNS-запросов с компьютера (троян или ботнет)
- Выявление потоков по IP-адресам из базы данных «плохих» адресов

2 ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ

- Детектирование фактов использования ПО на рабочих местах: обращения к облачным хранилищам, онлайн-игры
- Детектирование использования пользователями сетей DarkNet (Tor, I2P)
- Выявление подозрительных сервисов (неопознанные СУБД, веб-сервера внутри сети)

КЕЙСЫ || 2

3 ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНОГО ВЗАИМОДЕЙСТВИЯ С ВНЕШНИМИ СЕТЯМИ

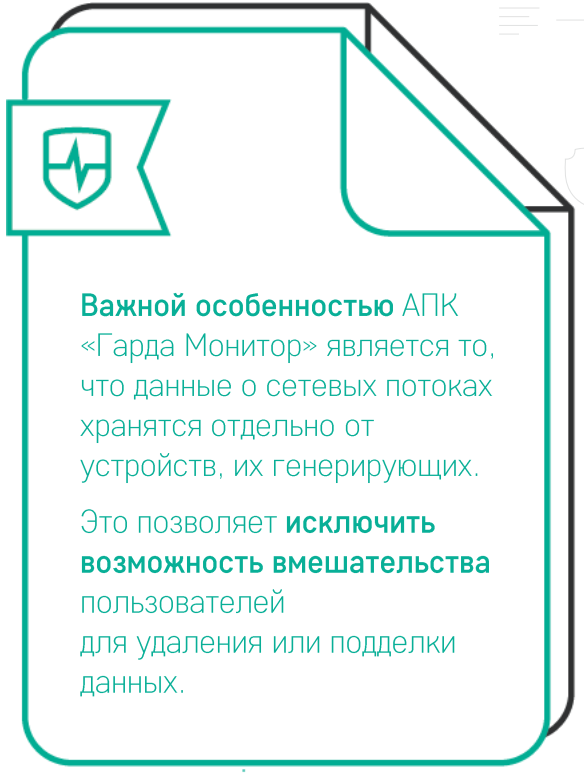
- Детектирование попыток удаленного доступа из внешних сетей к внутренним серверам
- Выявление VPN-каналов

4 ЛОГИРОВАНИЕ ПОТОКОВ ПО ВРЕМЕНИ

«Гарда Монитор» не только позволяет выявлять данные потоки, но также записывает их содержимое с привязкой ко времени.

Это позволяет:

- Выгрузить данные потоки в формате *.pcap
- Использовать эти потоки как доказательства в расследовании и суде



Важной особенностью АПК «Гарда Монитор» является то, что данные о сетевых потоках хранятся отдельно от устройств, их генерирующих.

Это позволяет **исключить возможность вмешательства** пользователей для удаления или подделки данных.

КЕЙСЫ || 3

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

5 СИГНАТУРНЫЙ АНАЛИЗ ТРАФИКА

- Выявление активности вредоносного и подозрительного ПО, эксплуатации уязвимостей
- Наличие собственной базы данных уязвимостей и экспертного центра
- Возможность выгрузки образцов сетевого трафика для последующего анализа
- Категорирование угроз
- Автоматизированные политики по выявлению угроз сетевой безопасности
- Детектирование фактов сетевой разведки
- Автоматическое обновление базы данных сигнатур

6 ПРОФИЛИРОВАНИЕ И ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА

- Построение поведенческой модели по политикам контроля сетевого трафика
- Выявление отклонений по объему потоков, количеству и другим параметрам

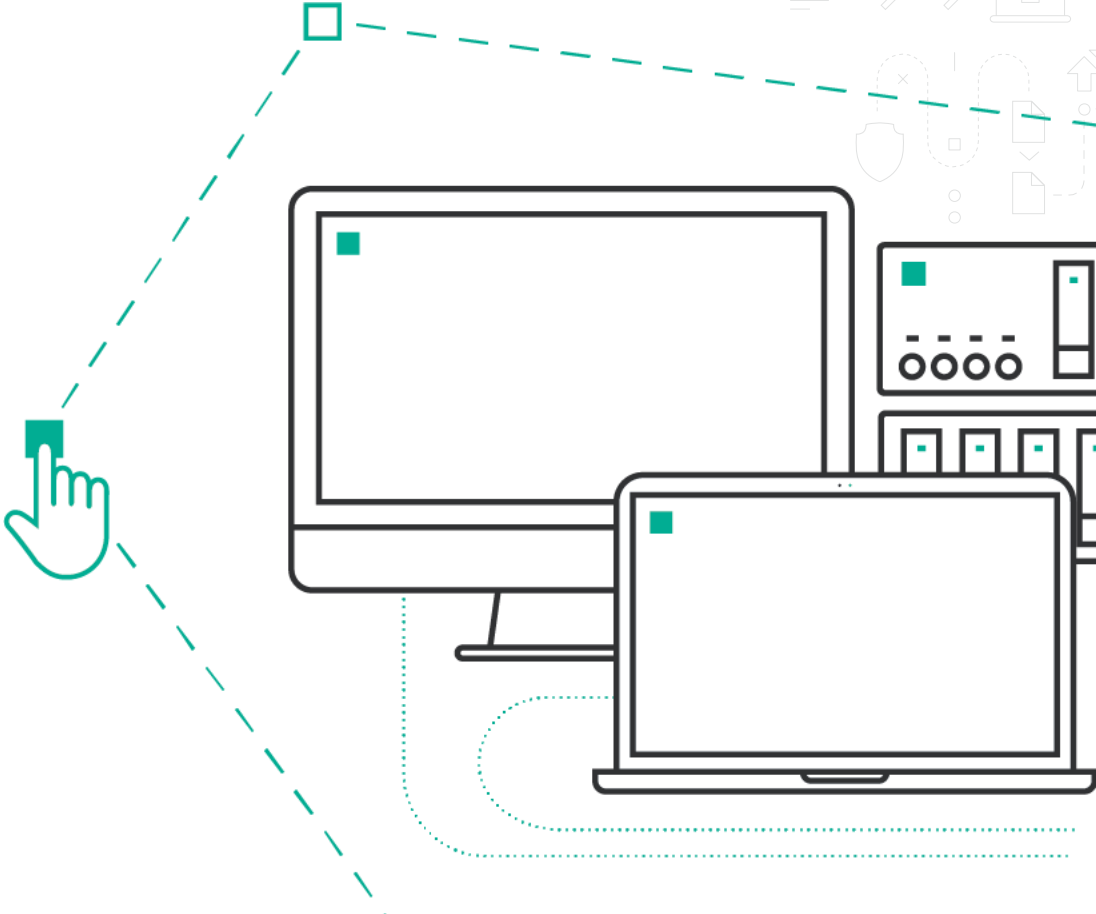
Примеры:

- Аномально большое количество DNS запросов от хоста
- Аномально большой объем данных, передаваемых по SSH за периметр
- Аномальное количество отправляемой почты с хоста или сервера

ГАРДА МОНИТОР ГАРДА ТЕХНОЛОГИИ

КОНТРОЛЬ «ВНЕШНЕГО ПЕРИМЕТРА» & ВЫЯВЛЕНИЕ УГРОЗ ИБ

- DoS-атаки (SYN-flood, ICMP-flood)
- Сканирование портов
- Сканирование хостов
- Обнаружение фактов подключения «извне» к точкам, не входящим во внешний периметр
- Указание точек внешнего периметра



ПОЛИТИКИ

ГАРДА МОНИТОР ГАРДА ТЕХНОЛОГИИ

КЛАССИФИКАЦИЯ ТРАФИКА (СВЫШЕ 250 ПРОТОКОЛОВ, БОЛЕЕ 30 СЕТЕВЫХ ПАРАМЕТРОВ)

БОЛЬШОЙ СПИСОК ПРЕДУСТАНОВЛЕННЫХ ПОНЯТНЫХ И ПОЛЕЗНЫХ ПОЛИТИК

- Обращение к скомпрометированному IP-адресу и с него
- Обращение к скомпрометированному Host'у/URL'у
- Попытка DNS-резолва скомпрометированного Host'а
- Использование TOR, VPN
- Использование ПО для удаленного доступа
- «Нерабочий» траффик (Игры, соц. сети)
- Рекомендации FinCERT
- Факты «Сетевой разведки»

ШИРОКИЕ ВОЗМОЖНОСТИ ПО ПОСТРОЕНИЮ ПОЛИТИКИ

- IP-адреса (включая группы) и порт
- MAC-адрес
- DNS-имя
- Тип протокола
- Длительность, размер потока
- Данные геолокации («Source-Destination»)
- Учетная запись, почтовый адрес, URL и другие
- Направление (входящий\исходящий)
- HTTP-метод
- Наличие вложений
- Ключевые слова в содержимом потока

Детектирование протоколов Darknet, P2P, аутентификации, облачных сервисов, протоколов удаленного доступа, SSH, HTTP(S), почтовых протоколов и т.д.

АНАЛИТИКА & ПОЛНОТЕКСТОВЫЙ ПОИСК ПО ПЕРЕХВАЧЕННЫМ ДАННЫМ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

АНАЛИТИЧЕСКИЕ ВОЗМОЖНОСТИ

Карта сети

Отображение карты сетевых взаимодействий и экспертного анализа над связями (визуализация, инфографика)

Entity Behavior Analytics (EBA)

Построение профилей сетевой работы устройств, выявление аномалий в поведении и существенных отклонений от «типового» поведения.

ПРИМЕРЫ КРИТЕРИЕВ ПОИСКА

- По IP-адресам источника и получателя
- По портам источника и получателя
- По типу протокола транспортного уровня
- По типу прикладного протокола
- По имени рабочей станции
- По Vlan ID
- По MAC-адресам источника и получателя

КОНСТРУКТОР ОТЧЁТОВ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ДЛЯ ЛЕГКОГО ВЕРХНЕУРОВНЕВОГО АНАЛИЗА СЕТЕВОЙ АКТИВНОСТИ РАЗНООБРАЗНЫЕ ОТЧЁТЫ СТРОЯТСЯ В РЕАЛЬНОМ ВРЕМЕНИ В ПРОСТОМ И ПОНЯТНОМ ГРАФИЧЕСКОМ ИНТЕРФЕЙСЕ

ДОСТУПНЫЕ ВИДЫ ОТЧЁТНОСТИ:

- Графические статистические отчёты
- Предустановленные шаблоны отчётов
- Построение отчётов по отобранным данным и временным рамкам

ИНТЕГРАЦИЯ И ЭКСПОРТ-ИМПОРТ

ГАРДА МОНИТОР ГАРДА ТЕХНОЛОГИИ

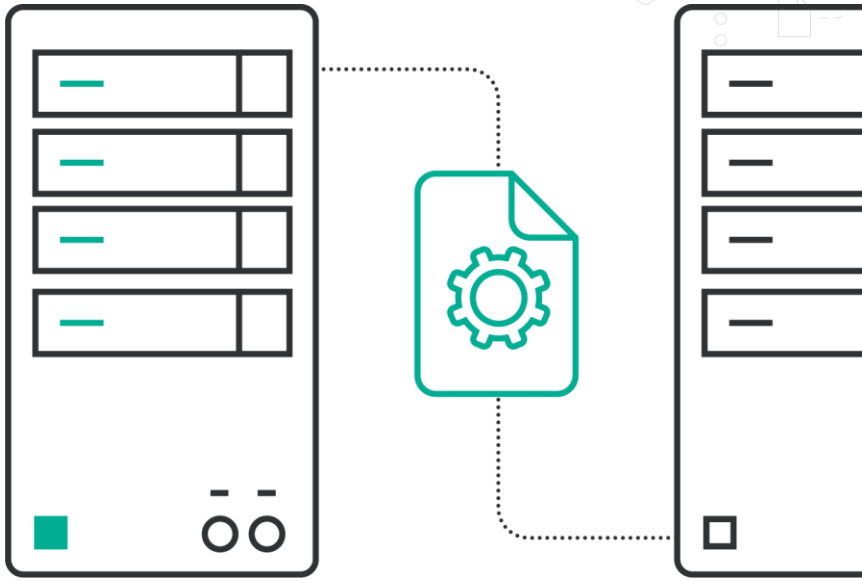
ДЛЯ ИНТЕГРАЦИИ С SIEM-СИСТЕМАМИ И МЕЖДУНАРОДНЫМИ БАЗАМИ ИНФОРМАЦИИ ПРЕДУСМОТРЕНА ВОЗМОЖНОСТЬ ЭКСПОРТА И ИМПОРТА ИНФОРМАЦИИ В РАЗЛИЧНЫХ ВИДАХ

ДОСТУПНЫЕ ФОРМЫ

- CSV
- XML
- PDF
- SysLog
- Электронная почта

МИРОВЫЕ БАЗЫ

- Базы репутации IP-адресов
- Базы скомпрометированных сайтов
- Базы скомпрометированных e-mail адресов (Спам, фишинг)



ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ РЕШЕНИЯ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

КОМПЛЕКС НАСТРОЕН И ГОТОВ К РАБОТЕ СРАЗУ ПОСЛЕ ИНСТАЛЛЯЦИИ (ИЗ КОРОБКИ)

Политики, правила, автоматическое обновление сигнатур и репутационные списки и пр .

РАСПРЕДЕЛЕННАЯ АРХИТЕКТУРА: МОНИТОРИНГ ТРАФИКА ВСЕХ ФИЛИАЛОВ КОМПАНИИ ИЗ ЕДИНОГО ЦЕНТРА

Гибкие политики безопасности как для всего гео-кластера, так и на конкретные филиалы.

ГИБКАЯ СИСТЕМА ФИЛЬТРОВ

Многокритериальный поиск в реальном времени

МАСШТАБИРУЕМОСТЬ КОМПЛЕКСА

Неограниченный объем записи трафика и оперативный доступ к данным за любой период времени

МНОЖЕСТВО СПОСОБОВ ПОДАЧИ ТРАФИКА

SPAN, NetFlow, Агенты, GRE

ПРОЗРАЧНОСТЬ СЕТЕВЫХ ПОТОКОВ ДАННЫХ

Полная картина происходящего в сети

КОМБИНАЦИЯ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ И ОБНАРУЖЕНИЯ СЕТЕВЫХ ИНЦИДЕНТОВ

На основе сигнатурного анализа, поведенческого анализа, детектирования по спискам

УДОБНЫЙ ИНТЕРФЕЙС

Гибкие отчеты, дашборды, статистика по трафику, гибкий поиск с функциональной строкой

КОМПЛЕКС НЕ ТРЕБУЕТ СТОРОННИХ ЛИЦЕНЗИЙ

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ || 1

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ПЕРЕДАЧА ДАННЫХ

- HTTPS
- HTTP
- WAP
- FTP
- TFTP
- SMB
- BitTorent
- Filetopia
- iMESH
- OpenFT
- Kazaa/Fasttrack
- eDonkey
- DirectConnect
- AppleJuice
- PANDO
- StealthNet
- AFP (Apple Filing Protocol, AppleShare)

ОБМЕН СООБЩЕНИЯМИ

- OSCAR (ICQ v7, v8, v9)
- IRC (Согласно RFC 2810-2813)
- MMP (Mail.Ru Агент)
- XMPP (QIP, Jabber)
- Tencent (QQ)
- MSN
- Yahoo
- MEEBO
- Skype
- WhatsApp
- Viber

АВТОРИЗАЦИЯ

- RADIUS
- TACACS+
- Diameter
- Kerberos

БАЗЫ ДАННЫХ

- PostgreSQL
- MySQL
- TDS
- MSSQL
- ORACLE
- Redis

СЕТЕВЫЕ СЛУЖБЫ

- RTP
- RTCP
- DNS
- SNMP
- SSH
- RDP
- RFB (VNC)
- NNTP
- MGCP
- TOR
- Opera Mini

ПРИВАТНЫЕ СЕТИ

- OpenVPN
- CiscoVPN
- HotspotShield VPN

ПОЧТОВЫЕ ПРОТОКОЛЫ

- SMTP
- IMAP4
- POP3
- NNTP
- MS Exchange (MAPI)

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ || 2

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ИГРЫ & РАЗВЛЕЧЕНИЯ

- XBOX
- Steam
- Battlefield
- Quake
- Halflife2
- World of Warcraft
- WARCRAFT3
- Stracraft
- Armagetron
- World of Kung Fu
- Guildwars
- Florensia
- Dofus
- CrossFire

ОБМЕН СООБЩЕНИЯМИ

- OSCAR (ICQ v7, v8, v9)
- IRC (Согласно RFC 2810-2813)
- MMP (Mail.Ru Агент)
- XMPP (QIP, Jabber)
- Tencent (QQ)
- MSN
- Yahoo
- MEEBO
- Skype
- WhatsApp
- Viber

УДАЛЁННОЕ УПРАВЛЕНИЕ

- SSH
- TeamViewer
- RDP
- VNC
- PCAnywhere

МУЛЬТИМЕДИА

- RealMedia
- Windowsmedia
- Icecast
- PPLive
- PPStream
- Zattoo
- SHOUTCast
- SopCast
- TVAnts
- TVUplayer
- VeohTV
- QQLive
- GloboTV
- Deezer

VOIP

- SIP
- Megaco (H.248)
- H.323
- SCCP (SKINNY)
- MGCP
- IAX
- WhatsApp Voice
- Webex
- TeamSpeak

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ || 3

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ПРОЧИЕ ПРОТОКОЛЫ

- 99Taxi
- Aimini
- Apple (iMessage, FaceTime...)
- Apple iCloud
- Apple iTunes
- AVI
- BGP
- Citrix
- CitrixOnline & GotoMeeting
- CNN
- Collectd
- Corba
- DCE RPC
- DHCP
- DHCPv6
- DirectDownloadLink
- DNS
- DropBox
- EGP
- FaceBook
- Feidian
- Fiesta
- Flash
- GaduGadu
- Gmail
- Gnutella
- Google
- Google Maps
- GRE
- GTP
- I23V5
- ICMP
- ICMPv6
- IGMP
- Instagram
- IPP
- IPSEC
- KakaoTalk Voice and Chat
- Kontiki
- LDAP
- LLMNR
- LotusNotes
- MapleStory
- MDNS
- Microsoft Cloud Services
- MMS
- MOVE
- MPEG
- NETBIOS
- Netflix
- NetFlow_IPFIX
- NFS
- NOE
- NTP
- OFF
- OGG
- OpenSignal
- OSPF
- Popo
- PPTP
- QUIC
- QuickTime
- RemoteScan
- RSYNC
- RTCP
- RTP
- RTSP
- SAP
- SCTP
- sFlow
- Simet
- Snapchat
- SNMP
- Socrates
- Soulseek
- Spotify
- SSDP
- SSL
- STUN
- Syslog
- Telnet
- Teredo
- Thunder Webthunder
- TOR
- Truphone
- Tuenti
- Twitch
- Twitter
- UbuntuONE
- UPnP
- USENET
- VMware
- VRRP
- Whois-DAS
- Wikipedia
- WindowsUpdate
- WinMX
- XDMCP
- YouTube
- ZeroMQ

ГАРДА
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ!

Дмитрий Горлянский

Технический эксперт
Гарда Технологии **gardatech.ru**

d.gorlianskiy@gardatech.ru