ГАРДА
ТЕХНОЛОГИИ

ГАРДА ТЕХНОЛОГИИ

РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ТЕХНОЛОГИИ — РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

150+

Внедрений на территории России во всех отраслях

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.

ГАРДА ТЕХНОЛОГИИ ВХОДИТ В **ИКС ХОЛДИНГ:**

- Экосистема из более, чем 30 компаний
- 50+ бизнес-партнёров в России и за рубежом
- 1’000 B2B клиентов более чем в 20 странах мира
- 6’000 высококвалифицированных специалистов
- Задачи государственного уровня: COVID-19 и другие

КОМПЛЕКСНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ И ВНЕШНИХ УГРОЗ

ГАРДА ТЕХНОЛОГИИ

ГАРДА АНАЛИТИКА

ПЛАТФОРМА ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

ГАРДА БД

АУДИТ И ЗАЩИТА БАЗ ДАННЫХ И ВЕБ-ПРИЛОЖЕНИЙ

ГАРДА МОНИТОР

ВЫЯВЛЕНИЕ И РАССЛЕДОВАНИЕ СЕТЕВЫХ ИНЦИДЕНТОВ

ГАРДА ПРЕДПРИЯТИЕ

КОНТРОЛЬ И АНАЛИЗ ИНФОРМАЦИОННЫХ ПОТОКОВ КОМПАНИИ

ФРОД ИНДЕКС

БОРЬБА С МОШЕННИЧЕСТВОМ И ГАРАНТИРОВАНИЕ ДОХОДОВ ОПЕРАТОРОВ СВЯЗИ

ПЕРИМЕТР

ПРЕДУПРЕЖДЕНИЕ, ОБНАРУЖЕНИЕ И ПОДАВЛЕНИЕ DDOS-АТАК

ГАРДА ФИЛЬТР

ОГРАНИЧЕНИЕ ДОСТУПА К ДОМЕНАМ, УКАЗАТЕЛЯМ СТРАНИЦ САЙТОВ И СЕТЕВЫМ АДРЕСАМ

АНТИ БОТНЕТ

ВЫЯВЛЕНИЕ ВРЕДОНОСНОЙ АКТИВНОСТИ В СЕТИ ОПЕРАТОРА СВЯЗИ И УЧАСТНИКОВ БОТ-СЕТЕЙ

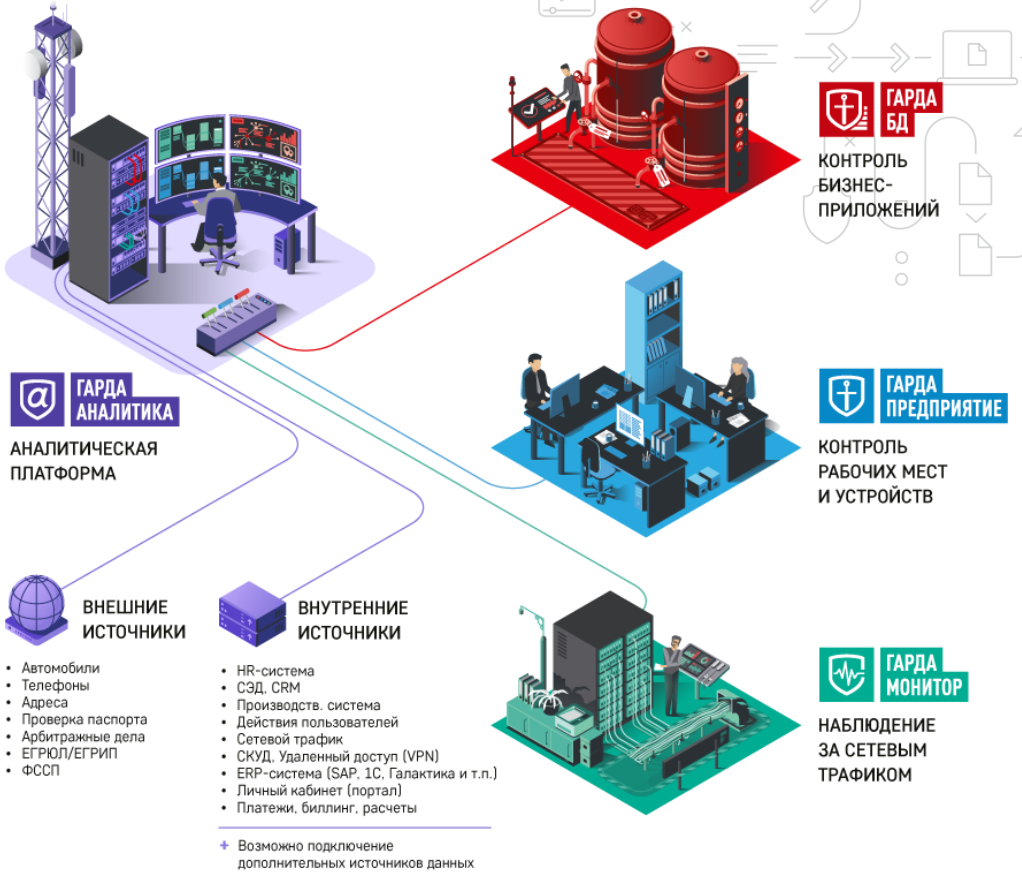
ЭКОСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГАРДА ТЕХНОЛОГИИ

АНАЛИТИЧЕСКАЯ ПЛАТФОРМА «ГАРДА АНАЛИТИКА» — ОСНОВА ЭКОСИСТЕМЫ БЕЗОПАСНОСТИ

- Позволяет оперативно создавать всесторонний комплекс защиты организации от угроз информационной и экономической безопасности
- Осуществляет защиту информации на уровнях сети, баз данных, рабочих местах и устройствах
- Минимизирует затраты на внедрение систем безопасности

80% ВСЕХ УГРОЗ БЕЗОПАСНОСТИ ДЕТЕКТИРУЕТСЯ **ВНУТРИ ПЕРИМЕТРА** ПРЕДПРИЯТИЯ

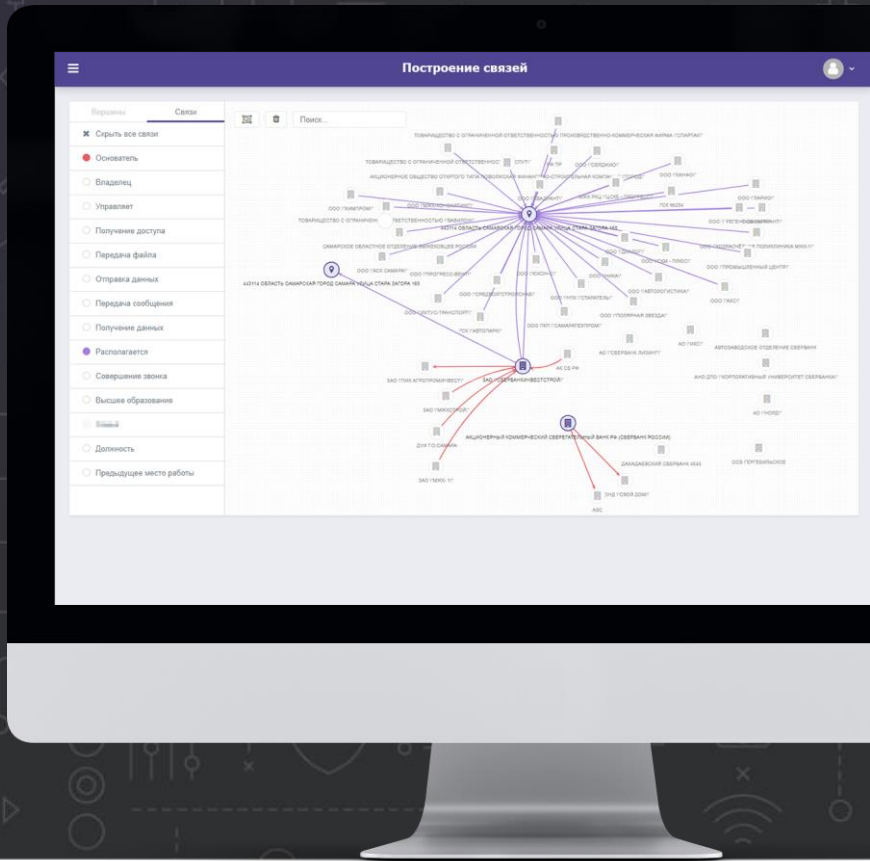


ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ПЛАТФОРМА ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

ПОСТРОЕНИЕ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ



ГАРДА АНАЛИТИКА — ИНФОРМАЦИОННОЕ ЯДРО БЕЗОПАСНОСТИ

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

- Строит интерактивное досье на людей и компании
- Связывает факты и события, полученные из множества баз данных
- Предиктивно сигнализирует об инцидентах, предотвращая возможный реальный ущерб
- Система открыта для подключения новых источников данных

Внутренние источники

- Кадровый учет
- Пропускная система
- Электронный документооборот
- Бухгалтерия
- Управление предприятием (1С, SAP)
- Производственная система
- ...
- и другие внутренние системы предприятия

Внешние открытые публичные источники

- Соц. сети
- Автомобили
- Телефоны
- Адреса
- Проверка паспорта
- Арбитражные дела
- ЕГРЮЛ/ЕГРИП
- Исполнительные дела

Иные источники

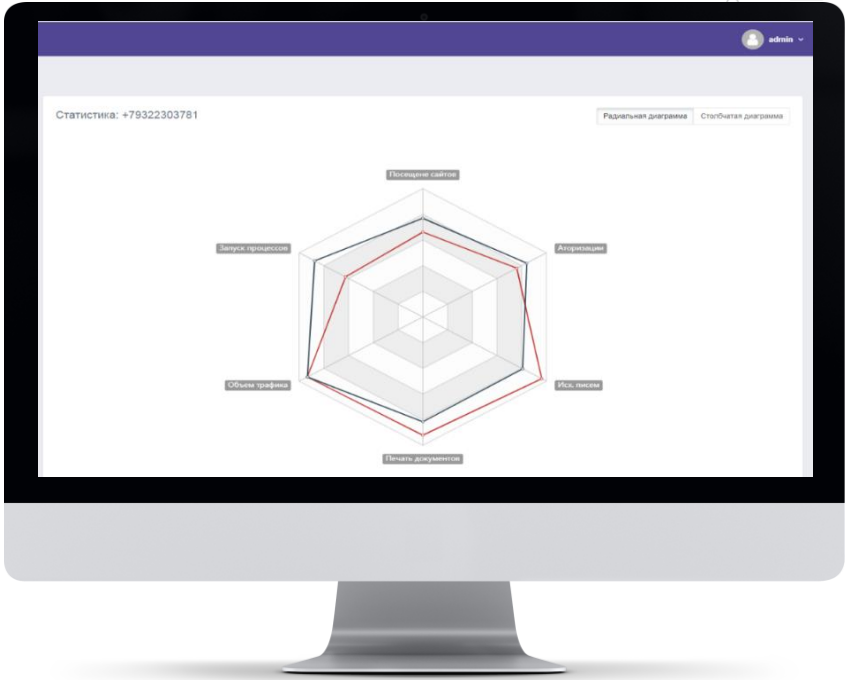
ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

АЛГОРИТМЫ МАШИННОГО ОБУЧЕНИЯ И ПРОФИЛИ ПОВЕДЕНИЯ

КЛЮЧЕВАЯ ЗАДАЧА СИСТЕМЫ — ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ НА РАННИХ СТАДИЯХ ДО ПРИЧИНЕНИЯ РЕАЛЬНОГО УЩЕРБА И ПРЕДИКТИВНАЯ КРИМИНАЛИСТИКА

- В систему заложено более 100 моделей, которые выявляют схемы мошенников в режиме «реального времени» с учетом отраслей и видов бизнеса
- Система анализирует рабочую активность сотрудников (бухгалтер, конструктор, инженер) и отслеживает отклонения от нормального поведения
- Благодаря технологиям искусственного интеллекта система постоянно обучается, совершенствуется, что позволяет выявлять неизвестные ранее схемы обхода процедур безопасности
- Интерфейс системы не требует специальных технических навыков



МЕСТОПОЛОЖЕНИЕ И ОБЩЕНИЕ

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ДАННЫЕ О МЕСТОПОЛОЖЕНИИ И КОММУНИКАЦИЯХ СЛУЖЕБНЫХ НОМЕРОВ ИЛИ УСТРОЙСТВ

- Перемещение по большим площадям (полям, участкам)
- Регулярное нахождение на неразрешенной территории
- Совместное местонахождение, передвижение и общение
- Отклонения от привычных маршрутов, контроль логистики

ПРИМЕР

Эксклюзивные сорта фруктов (завезенные саженцы)

Огороженная территория

+

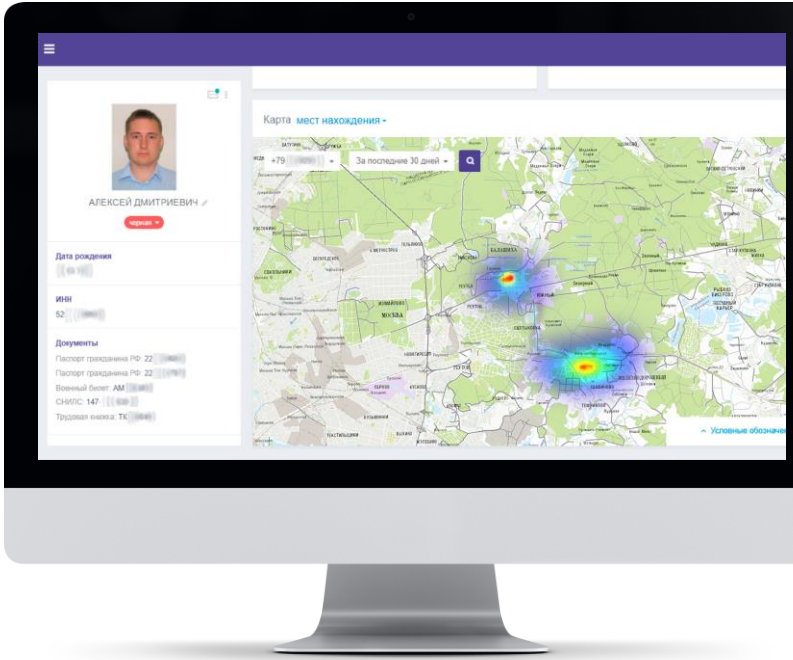
СКУД

Видеоаналитика с камер

Данные с дронов

«Умные» каски (чипы на одежде)

Это всё можно загрузить в Аналитику, которая соберет из разрозненных фактов реальный инцидент



СФЕРЫ ПРИМЕНЕНИЯ

ТЕЛЕКОМ

- Телекоммуникационное мошенничество
- Анализ финансовых операций

СТРАХОВЫЕ КОМПАНИИ

- Оформление страховых полисов по недостоверным данным
- Недобросовестные внешние эксперты (оценщики, судебные и т.п.)
- Урегулирование убытков по сфальсифицированным страховым случаям

ТЭК

- Мошенничества с присоединением потребителей и оплатой
- Мониторинг безопасности процессов генерации, добычи, транспортировки, передачи

ПРОМЫШЛЕННОСТЬ

- Распространение конструкторской документации, производственных секретов
- Нарушения производственных и бизнес-процессов
- Мошенничество при сбыте

В РАБОТЕ СОТРУДНИКОВ

- Мониторинг общения сотрудников по корпоративным sim-картам и корпоративным устройствам
- Выявление отклонений от привычных маршрутов следования сотрудников

ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

- Внутреннее мошенничество (сотрудники)
- Противодействие отмыванию доходов (ПОД/ФТ, AML, теневые операции)

ГОСУДАРСТВЕННЫЕ СИСТЕМЫ

- Злоупотребления при оказании государственных услуг
- Поддержка безопасности процессов государственного управления и обеспечения правопорядка

РИТЕЙЛ

- Махинации с поставками
- Мошенничества в интернет-магазине
- Нарушения в процессах функционирования складов, торговых залов, кассовых узлов

В СФЕРЕ СНАБЖЕНИЯ

- Выявление махинаций с поставками
- Манипулирование тендерами и закупками
- Нарушения при проводках и обороте товарно-материальных ценностей

БЕЗОПАСНОСТЬ ОБЪЕКТОВ КИИ

- Обеспечение мер, предусмотренных федеральным законом №187, его подзаконными актами
- Мониторинг угроз и инцидентов, в том числе в технологических сегментах

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

DLP-СИСТЕМА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

КОНТРОЛЬ И АНАЛИЗ ИНФОРМАЦИОННЫХ ПОТОКОВ КОМПАНИИ, ЗАЩИТА И ПРЕДОТВРАЩЕНИЕ УТЕЧЕК КОНФИДЕНЦИОАНОЙ ИНФОРМАЦИИ

ОБЗОР РЕШЕНИЯ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

«ГАРДА ПРЕДПРИЯТИЕ» НА ЗАЩИТЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ:

- Контролирует выполнение политик безопасности
- Защищает потенциальные каналы утечки информации
- Осуществляет контроль работы сотрудников

Система выявляет нарушения и угрозы информационной безопасности сразу после запуска, до завершения всех этапов внедрения и настройки DLP*

** (Data Loss Prevention – Защита от утечек информации)*

ОБЛАСТИ ПРИМЕНЕНИЯ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

СИСТЕМА АВТОМАТИЗИРУЕТ РУТИННУЮ РАБОТУ И ПОЗВОЛЯЕТ ВИДЕТЬ ПОЛНУЮ КАРТИНУ КОММУНИКАЦИЙ В ОРГАНИЗАЦИИ В ЛЮБОЙ МОМЕНТ ВРЕМЕНИ:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- Контроль информационных потоков компании
- Контроль рабочих мест сотрудников
- Отслеживание и предупреждение инцидентов ИБ
- Раннее обнаружение и предотвращение утечек информации
- Блокировка недопустимых действий
- Расследование инцидентов

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

- Мошеннические действия
- Сговоры среди сотрудников
- Работа на конкурентов
- Нецелевое расходование ресурсов компании
- Аналитическая поддержка при взаимодействии с правоохранительными органами

HR

- Контроль рабочего времени сотрудников
- Нелояльное отношение к организации
- Конфликтные ситуации в коллективе
- Поиск новой работы
- Социальные проблемы

ВСЕСТОРОННИЙ КОНТРОЛЬ ИНФОРМАЦИИ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ТОТАЛЬНЫЙ ПЕРЕХВАТ ДАННЫХ

Система перехватывает и накапливает данные со всех подключённых к ней информационных каналов компании

Выявляет причину, предшествующую инциденту, и его последствия, позволяя просмотреть действия сотрудников в ретроспективе

Фиксирует нарушения политик безопасности (в том числе по ранее накопленным данным), предоставляя широкие возможности при расследовании инцидентов

СВЕРХБЫСТРЫЙ ПОИСК

Поиск информации не зависит от типа файлов и возможен внутри архивов

Ретроспективный поиск данных по заданным параметрам

Сверхбыстрый поиск по всему объёму данных

ВИЗУАЛИЗАЦИЯ ИНФОРМАЦИИ В СИСТЕМЕ

Визуализация результатов поиска по различным параметрам

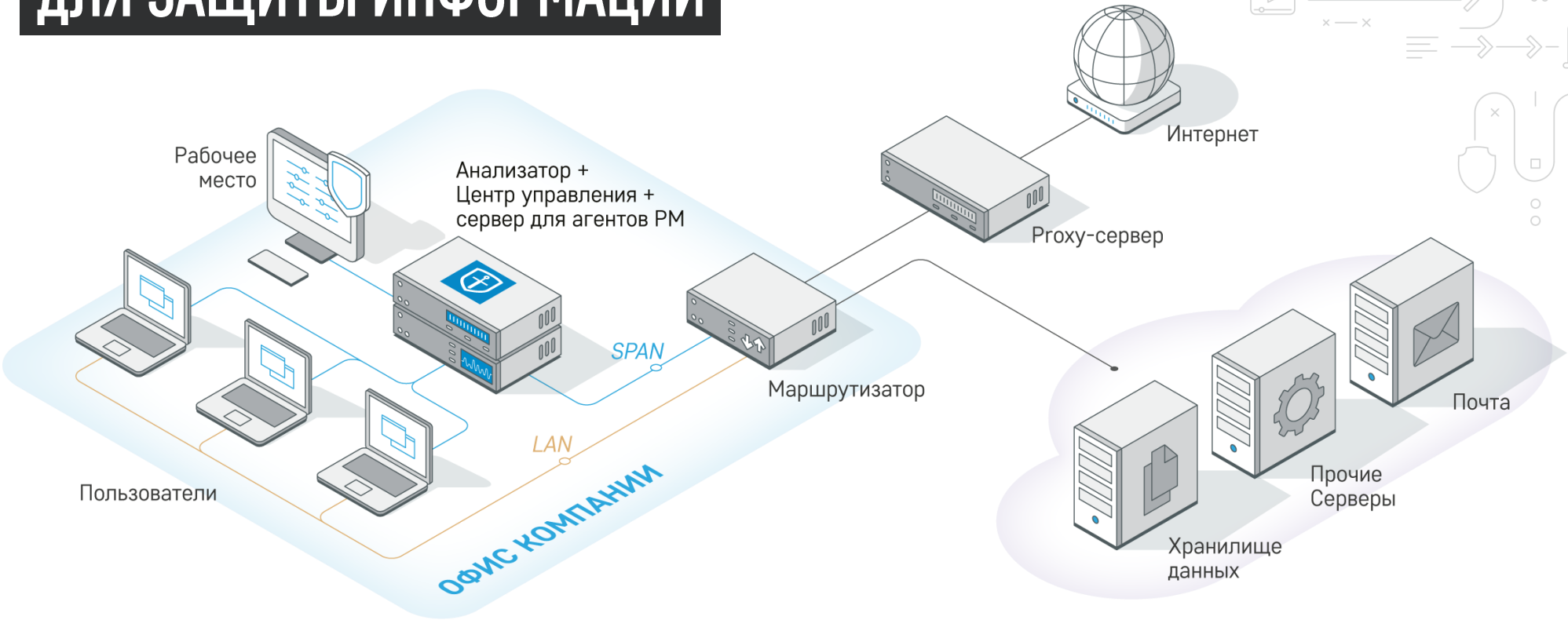
Интерактивные графики (Технология drill down)

Построение маршрутов утечки информации

СТРУКТУРА РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ



- ☑ Политики безопасности
- ☑ Быстрый поиск
- ☑ Хранение данных
- ☑ Декодирование трафика

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

АУДИТ И ЗАЩИТА БАЗ ДАННЫХ И БИЗНЕС-ПРИЛОЖЕНИЙ

- **Многоуровневый анализ сетевого трафика**
  выявит неконтролируемые базы данных и уязвимости в комплексе СУБД
- **Динамическое профилирование**
  на основе UEBA позволит вычислить подозрительные действия пользователей и выявить аномалии и отклонения их поведения
- **Интеллектуальная система отчётности**
  сделает расследование инцидентов простым и быстрым, а встроенная механика блокировок позволит предотвратить несанкционированный доступ к данным

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

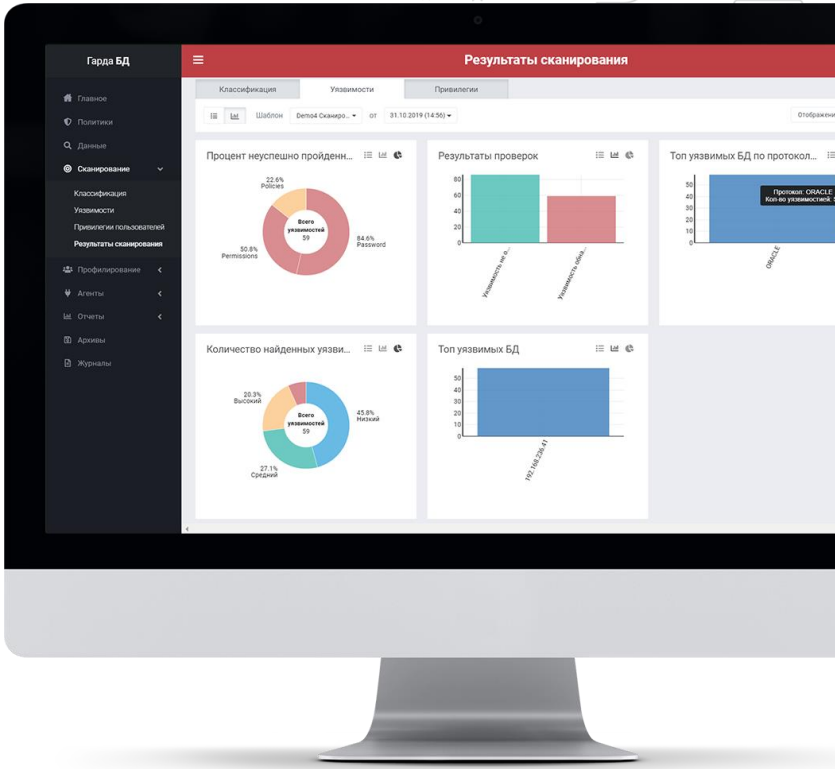
ГАРДА БД
ГАРДА ТЕХНОЛОГИИ

«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
- 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
- Контроль удаленного доступа сотрудников

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

- 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

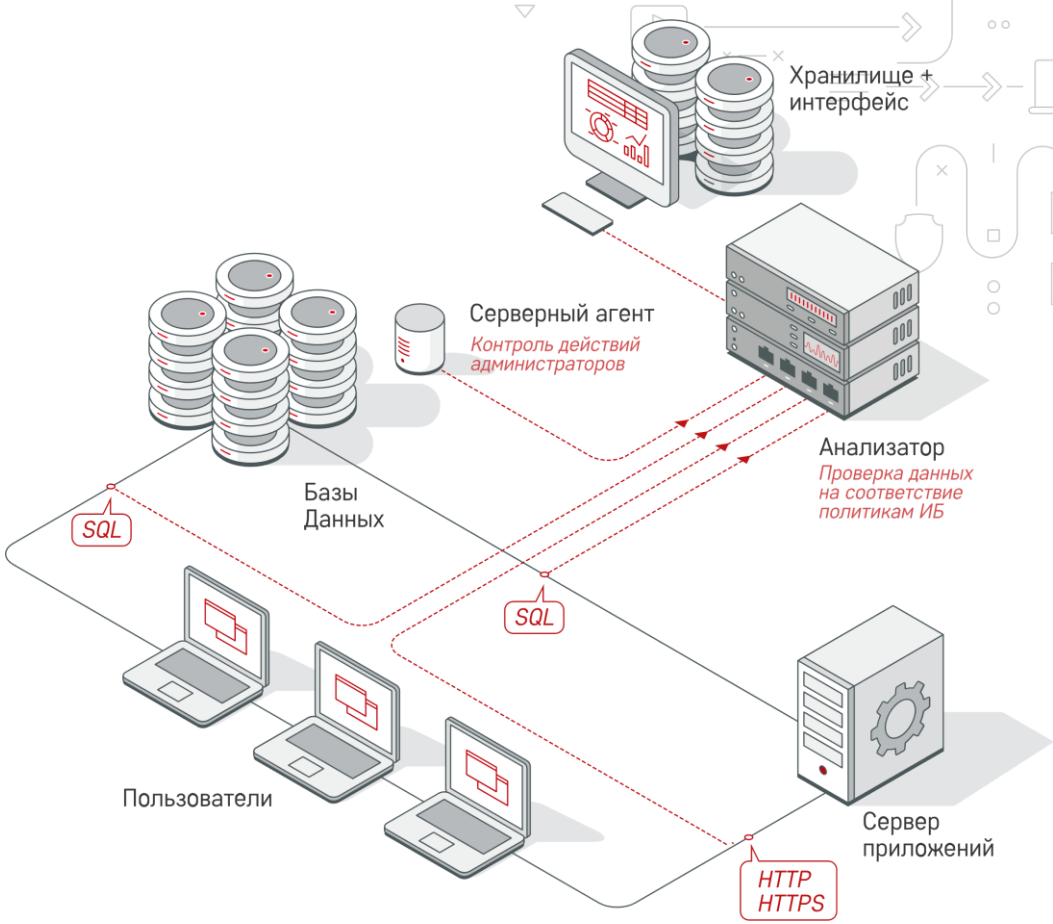


100 ТБ Поиск по хранилищам с размером свыше 100ТБ

10 ГБ/С Скорость анализа трафика более 10 Гбит/с

ПРИНЦИП РАБОТЫ

- Анализ сетевого трафика с возможностью мониторинга или блокировки нелегитимных запросов пользователей и получаемых данных из СУБД
- Обработка данных и долгосрочное хранение всех запросов и ответов для ретроспективного анализа
- Автоматический поиск новых СУБД, не стоящих на контроле, классификация их по типу хранимых данных
- Сканирование баз данных, находящихся под контролем
- Аналитическая отчетность и поведенческий анализ (UBA), выявление нарушений политик безопасности
- Система оповещения уведомляет о событиях по электронной почте, передает данные во внешние SIEM-системы, отображает отчёты на главном экране



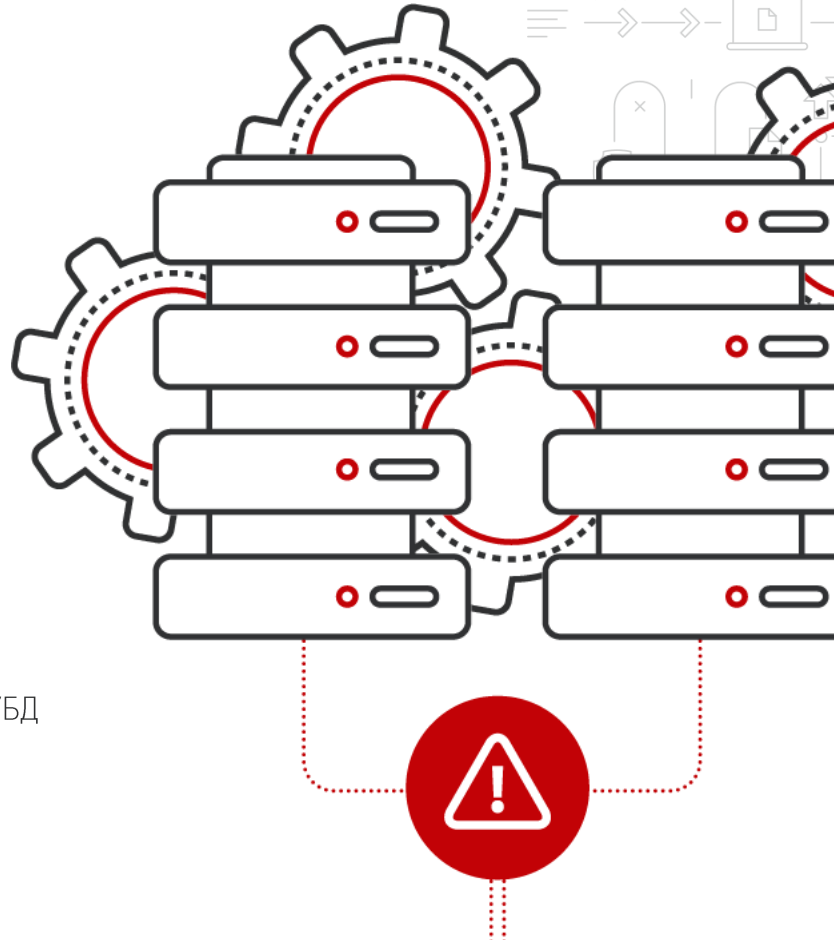
ПОМОГУТ ЛИ ШТАТНЫЕ СРЕДСТВА КОНТРОЛЯ?

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

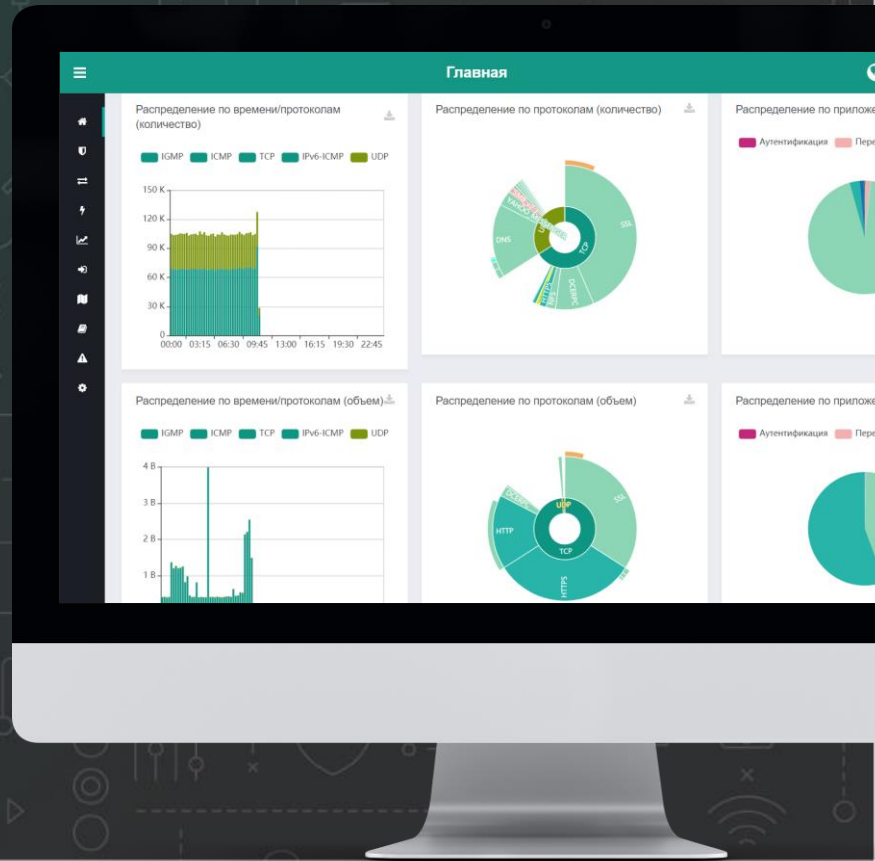


ГАРДА МОНИТОР

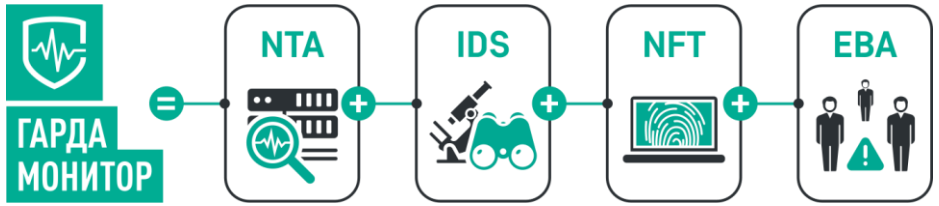
ГАРДА ТЕХНОЛОГИИ

ВЫЯВЛЕНИЕ УГРОЗ И РАССЛЕДОВАНИЕ СЕТЕВЫХ ИНЦИДЕНТОВ

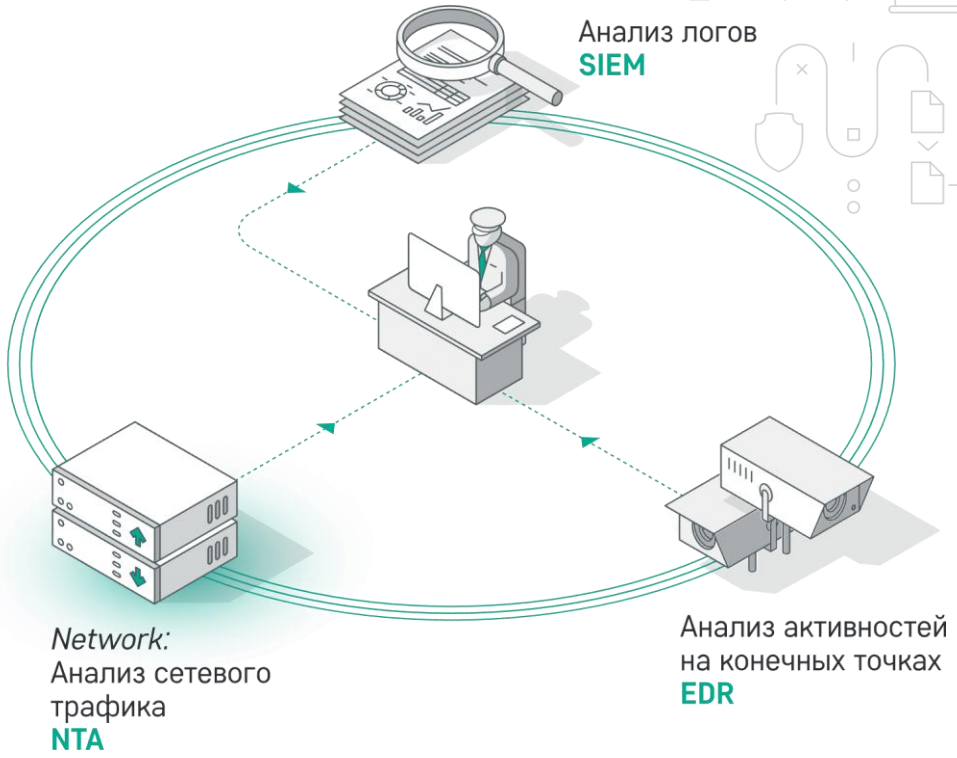
ОБНАРУЖЕНИЕ АТАК НА ПЕРИМЕТРЕ И ВНУТРИ СЕТИ



NTA — ПОЛНАЯ ПРОЗРАЧНОСТЬ СЕТИ



- Видеть сеть в крупной компании, когда недостаточно endpoint
- Защита от администраторов
- Когда антивирус – это уже поздно, а FW – пропустил угрозу
- Незаменим в расследованиях и при доказывании
- Поведенческий анализ по совокупности факторов
- 4+ технологии и все в одном окне
- Много нестандартных, мобильных или IoT устройств



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

Выявляет признаки вредоносного ПО
в сетевом трафике

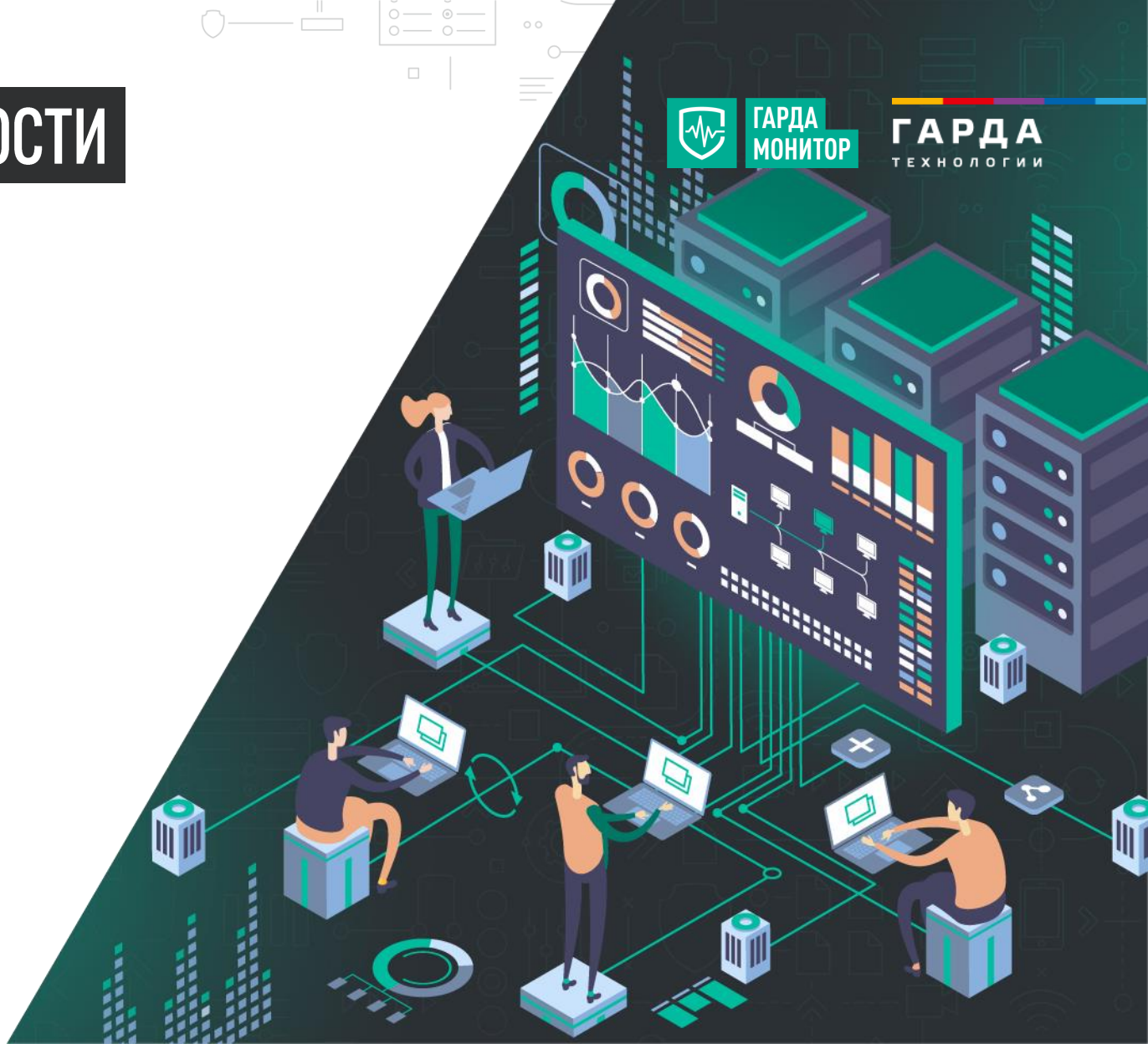
Осуществляет мониторинг
и сбор данных о сетевой активности

Выявляет атаки на периметре
и внутри сети

Обеспечивает **тотальную запись**
сетевых потоков

Анализирует события
сетевой безопасности

Позволяет выполнять **расследования**
сетевых инцидентов



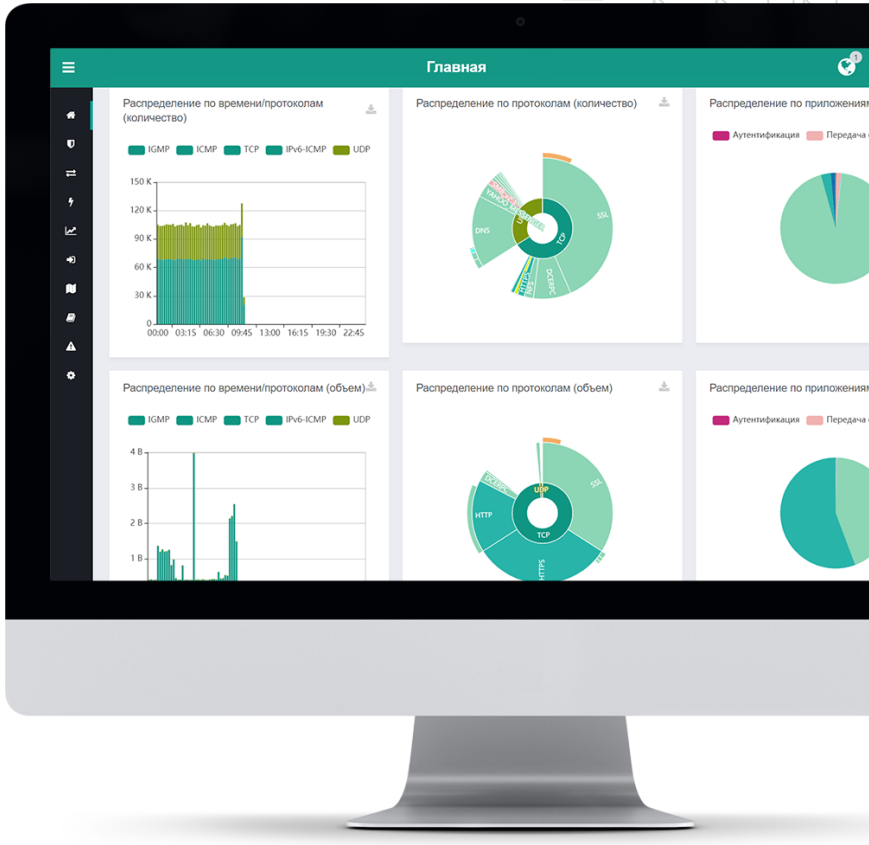
СФЕРЫ ПРИМЕНЕНИЯ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

«ГАРДА МОНИТОР» ПОВЫШАЕТ ЭФФЕКТИВНОСТЬ РАБОТЫ ЦЕНТРОВ МОНИТОРИНГА (SOC), ХОЛДИНГОВЫХ СТРУКТУР, ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ КОМПАНИЙ И ДРУГИХ СЕКТОРОВ БИЗНЕСА:

- Промышленные и производственные предприятия
- Государственный сектор
- Финансовые и инвестиционные компании
- IT-компании
- Телеком
- И другие



При установке система уже содержит подключенные и обновляемые базы сигнатур и репутационные списки

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

100 ТБ Хранение более 100 Тб трафика

10 ГБ/СЕК Анализ трафика 10 Гбит/с на модуль

250 ТИПОВ Классификация трафика свыше 250 типов протоколов

ПРИНЦИП РАБОТЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

КОНТРОЛЬ СЕТЕВЫХ КАНАЛОВ

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

ПЕРЕХВАТ, АНАЛИЗ И ЗАПИСЬ

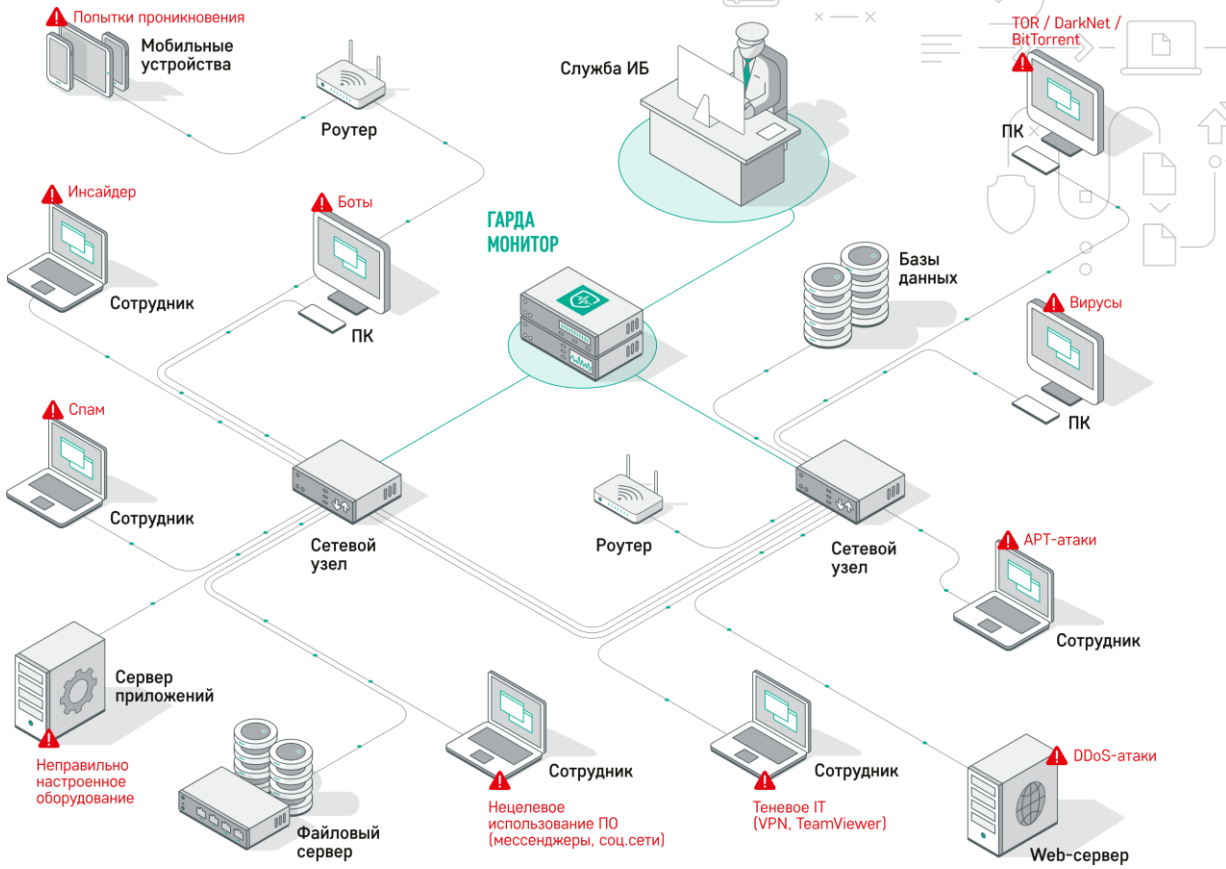
- IP-трафика в режиме реального времени

УДОБНЫЙ ВЕБ-ИНТЕРФЕЙС

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

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



ФРОД ИНДЕКС

ГАРДА ТЕХНОЛОГИИ

БОРЬБА С МОШЕННИЧЕСТВОМ И ГАРАНТИРОВАНИЕ ДОХОДОВ ОПЕРАТОРОВ СВЯЗИ

РЕШЕНИЕ ПО ПОСТРОЕНИЮ СИСТЕМ
ОПЕРАТОРСКОГО И НАЦИОНАЛЬНОГО УРОВНЯ
ПО БОРЬБЕ С ФРОДОМ В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ

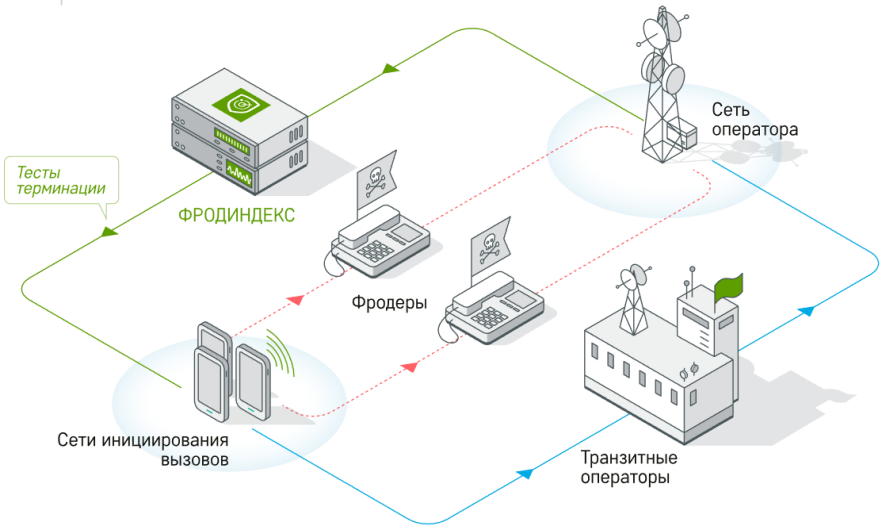
АНТИФРОД & REVENUE ASSURANCE

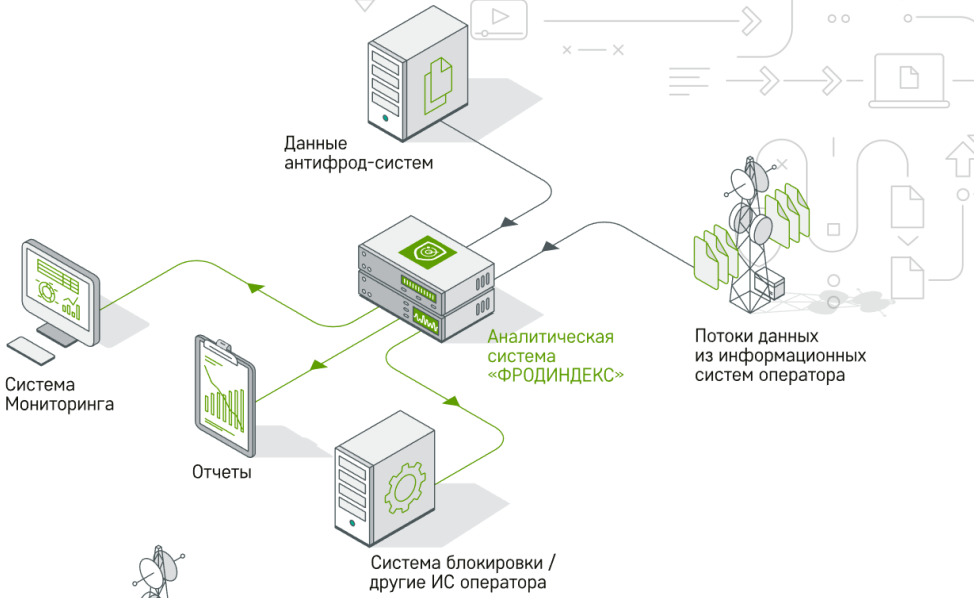
ФРОД ИНДЕКС

ГАРДА ТЕХНОЛОГИИ

- Контроль незаконной терминации международного голосового трафика на сети оператора связи
- Контроль трафика по приоритетам в междугородном и международном направлениях
- Контроль незаконного пропуска и рассылок SMS трафика
- Контроль потерь доходов компании и целостности данных в информационных системах оператора
- Фильтрация трафика

СХЕМЫ КОНТРОЛЬНЫХ ПРОЗВОНОВ



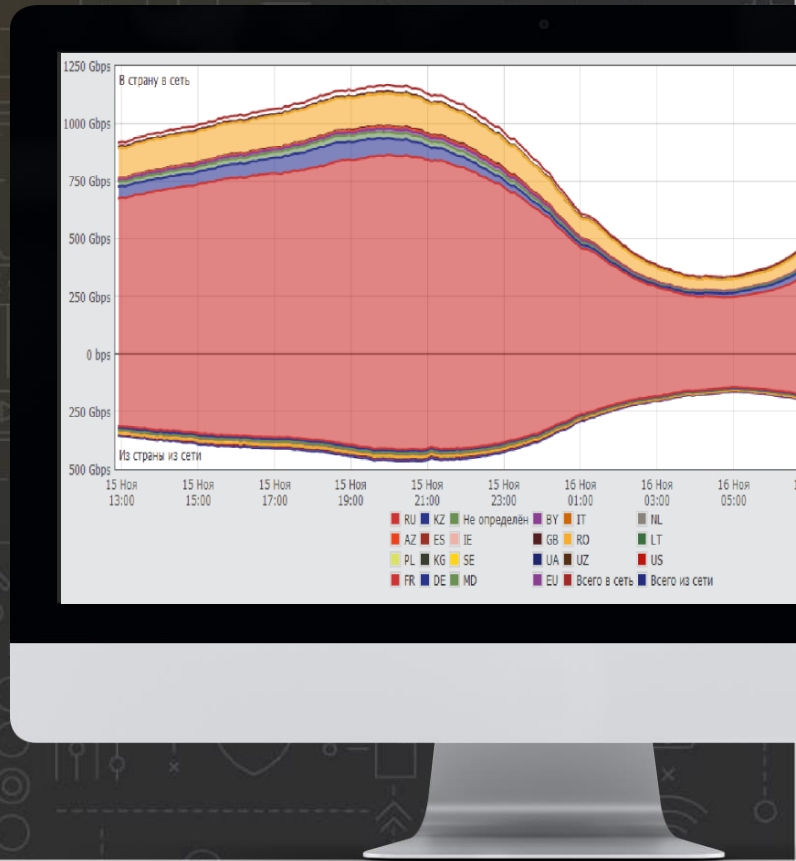


ПЕРИМЕТР

ГАРДА ТЕХНОЛОГИИ

ЗАЩИТА ОТ DDOS-АТАК

ГРУППА РЕШЕНИЙ ОПЕРАТОРСКОГО КЛАССА ДЛЯ ПРЕДУПРЕЖДЕНИЯ, ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ DDOS-АТАК РАЗЛИЧНОГО ТИПА В СЕТИ ПЕРЕДАЧИ ДАННЫХ И ЦОД ОПЕРАТОРА



ЗАЩИТА ОТ DDOS-АТАК

ПЕРИМЕТР ГАРДА ТЕХНОЛОГИИ

ОБНАРУЖЕНИЕ И ПОДАВЛЕНИЕ АТАК И АНОМАЛИЙ ТРАФИКА

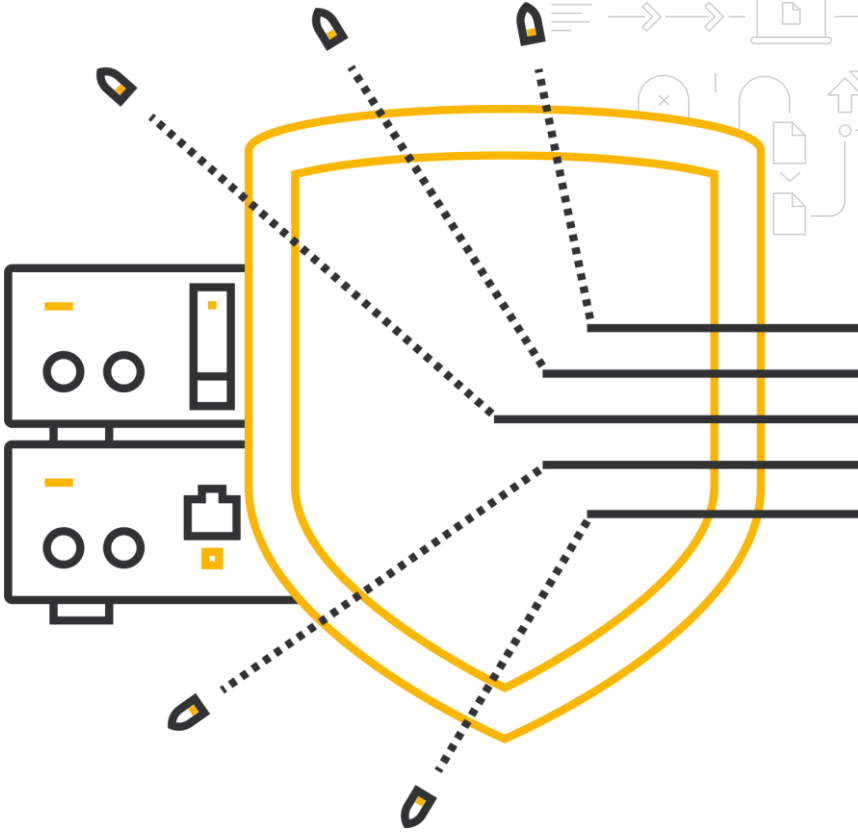
Детектирует большой спектр событий на устройствах сети, выявляет вредоносную активность на высоких скоростях и подавляет её

ОПТИМИЗАЦИЯ, ПЛАНИРОВАНИЕ И КОНТРОЛЬ СТРУКТУРЫ СЕТИ

Детальная информация о маршрутах прохождения трафика позволяет проводить оптимизацию внутренней структуры сети и межоператорского взаимодействия

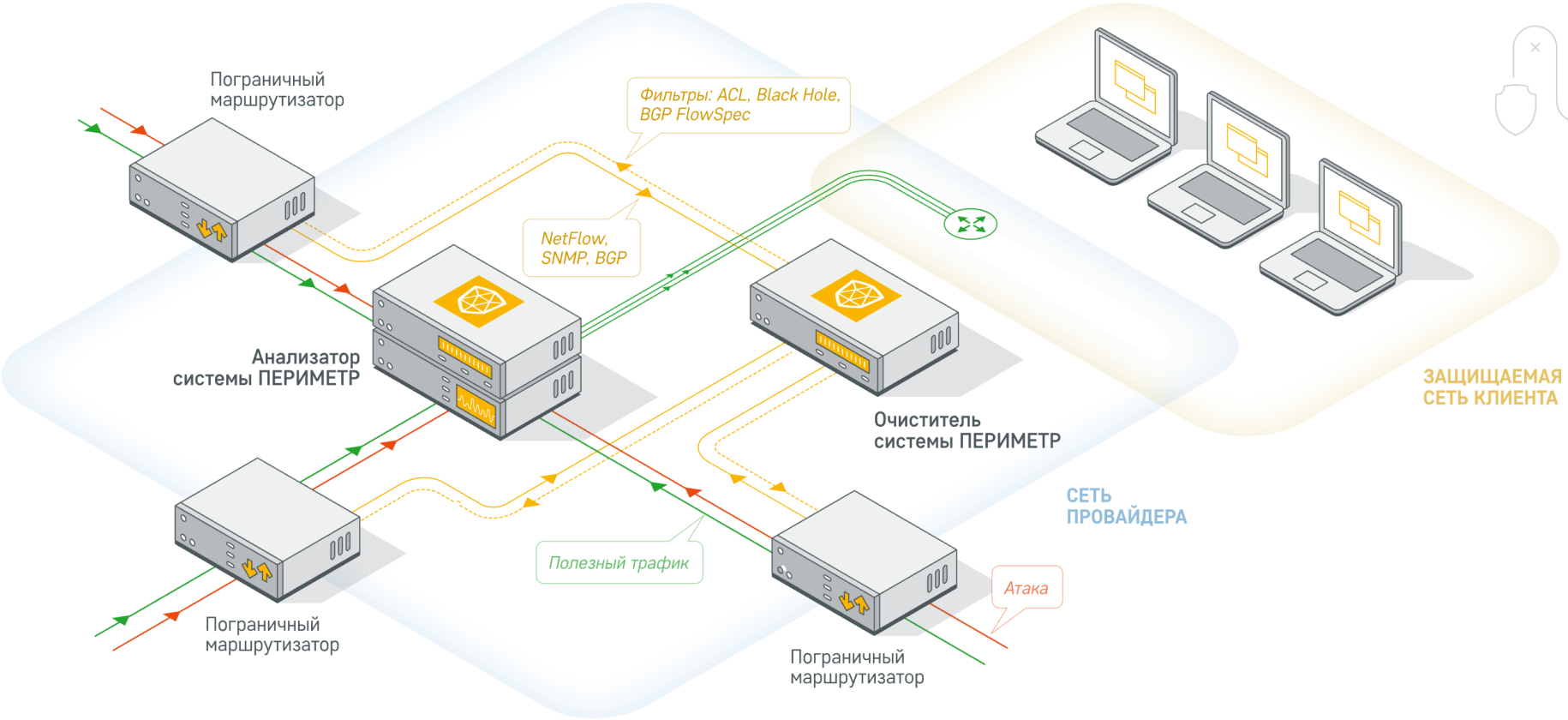
АНАЛИЗ «СЫРОГО» ТРАФИКА

Фильтруется именно зловредный трафик, а запросы добропорядочных пользователей беспрепятственно пропускаются



ПЕРИМЕТР ГАРДА ТЕХНОЛОГИИ

СТРУКТУРА РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ОТ DDOS-АТАК

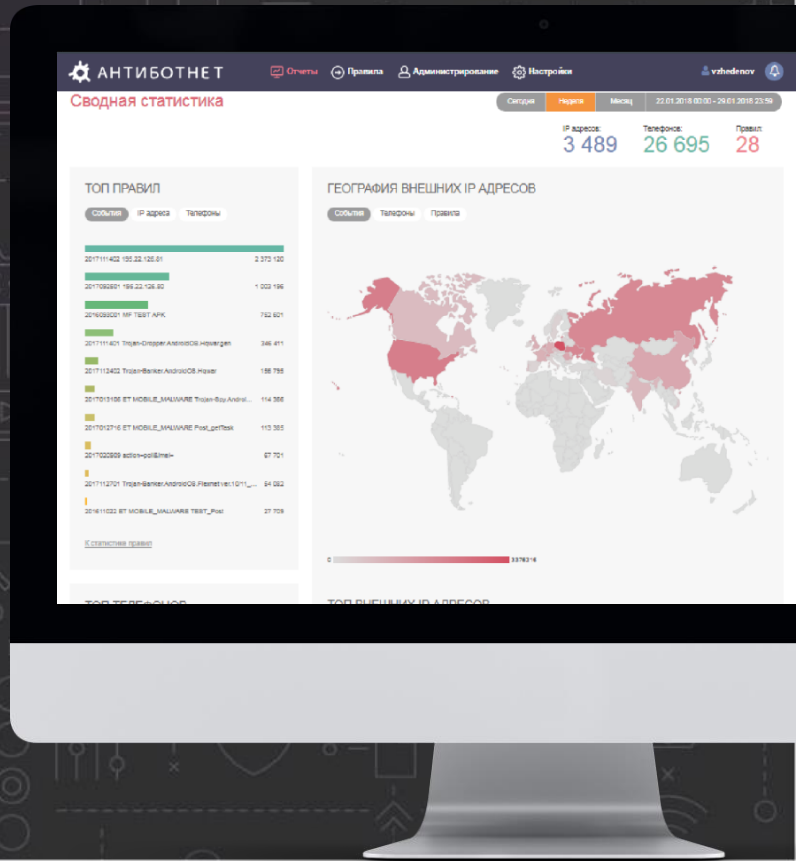


АНТИ
БОТНЕТ

ГАРДА
ТЕХНОЛОГИИ

ВЫЯВЛЕНИЕ ЗАРАЖЁННЫХ ТЕЛЕФОНОВ

РЕШЕНИЕ ДЛЯ ВЫЯВЛЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ В СЕТИ ОПЕРАТОРА СВЯЗИ И УЧАСТНИКОВ БОТ-СЕТЕЙ, ДЕЙСТВИЯ КОТОРЫХ НАПРАВЛЕНЫ ПРОТИВ АБОНЕНТОВ ОПЕРАТОРА



ВЫЯВЛЕНИЕ ЗАРАЖЁННЫХ ТЕЛЕФОНОВ

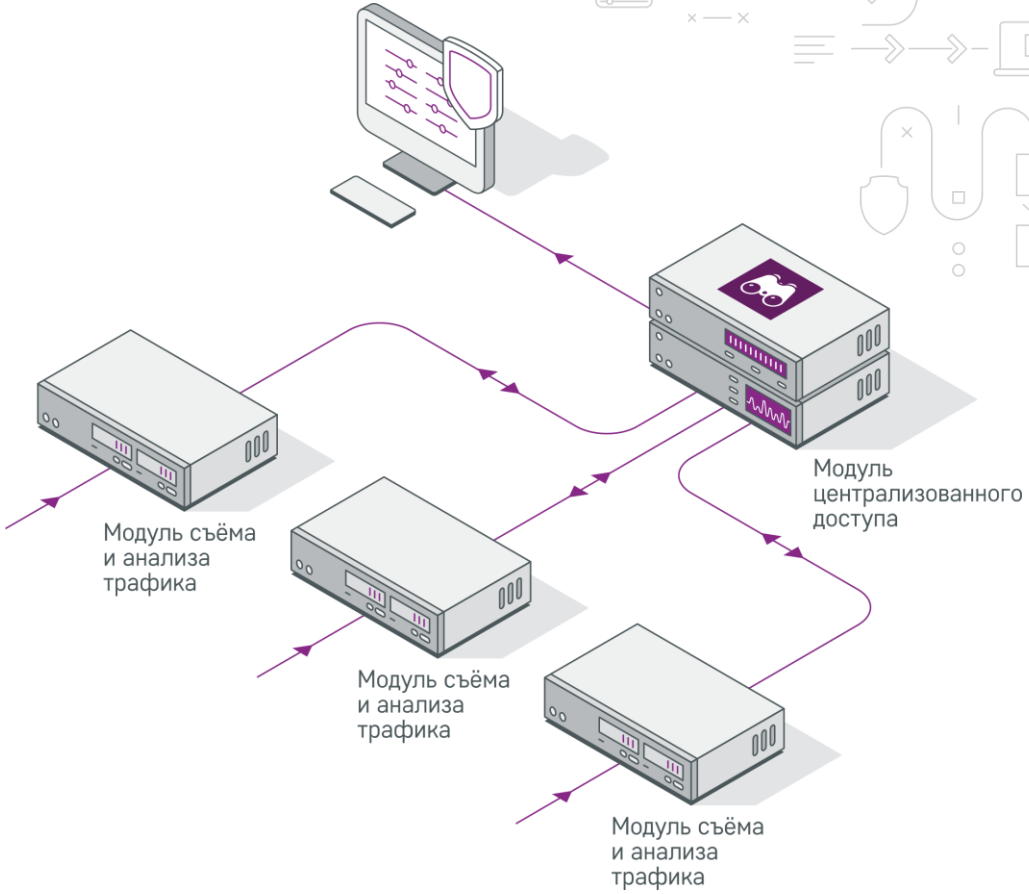
АНТИ БОТНЕТ ГАРДА ТЕХНОЛОГИИ

Мониторинг вредоносной активности бот-сетей в сети оператора связи:

- фактов вредоносной активности;
- зараженных телефонов;
- командных центров бот-сетей.

Запись фрагментов вредоносного трафика для последующего анализа.

Оператор может блокировать доступ к вредоносным ресурсам для защиты абонентов.



ГАРДА
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ!

г. Нижний Новгород, Пр. Гагарина, 50к9
8 (831) 422 12 21

г. Москва, Мичуринский пр., 27к5
8 (495) 540 05 27

/gardatechnologies

/garda_tech