ГАРДА МОНИТОР

Выявление и расследование сетевых инцидентов

ГАРДА
МОНИТОР

«Гарда Монитор» — это

программно-аппаратный комплекс класса сетевой форензики для анализа и расследования сетевых инцидентов.

Полный контроль сетевых потоков данных на предприятии

Гарда Монитор обеспечивает прозрачность сетевых потоков данных с помощью тотального контроля трафика сети компании в режиме реального времени, выявляет аномалии и помогает в расследовании инцидентов.

Контроль и анализ трафика

- Мониторинг IP-трафика локальных сетей и выявление сетевых инцидентов безопасности
- Анализ информационных потоков по всем актуальным протоколам
- Ведение архива объектов информационного обмена для ретроспективного анализа событий

Профессиональный подход к сетевой форензике

- Мониторинг сетевой активности крупных предприятий
- Работа центров по мониторингу и реагированию на инциденты
- Компьютерная криминалистика

Гарда Монитор в действии

Система обеспечивает тотальную запись сетевых потоков для эффективного анализа событий сетевой безопасности и помогает найти ответы на главные вопросы:

Что произошло?

Каждый день крупные компании сталкиваются с кибератаками, нарушениями прав доступа к конфиденциальной информации, заражениями вирусным ПО. Гарда Монитор в режиме реального времени выявит сетевую аномалию и отправит сигнал в службу информационной безопасности.

Как это произошло?

Расследование инцидентов с Гардой Монитор заменяет месяцы ручной работы. Запись всего трафика и возможность декодирования сообщений позволяет выявить причины аномалии и просмотреть каждый этап сетевой активности.

Что нужно сделать, чтобы инциденты не повторялись?

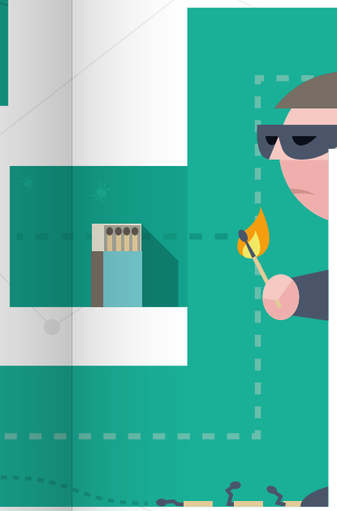
Когда файрвол пропустил инцидент, антивирус и другие системы безопасности не сработали вовремя, а местонахождение проблемы остается загадкой для службы безопасности — не все потеряно.

Что в опасности?

Гарда Монитор позволит быстро реагировать на инциденты благодаря наглядной локализации аномальных событий в сети.

Гарда Монитор — система последнего шанса

для выявления и расследования инцидентов на сети компании. Ретроспективный анализ трафика за любой период времени позволит оперативно решить проблему и создать политики безопасности для предотвращения подобных ситуаций в будущем.



Кто инициатор?

Запись трафика со всех необходимых каналов сети позволяет анализировать все инциденты по категориям и, сопоставив по времени, выявить инициатора. Если сетевой обмен осуществляется с узлами, находящимися за пределами компании, то Гарда Монитор определяет их географическое местоположение.

Принцип работы Гарды Монитор

Гарда Монитор работает с большим объемом неструктурированных данных — Big Data. Система быстрого поиска, функции анализа «сырого» трафика и высокопроизводительная система хранения собственной разработки МФИ Софт позволяют выявлять инциденты в режиме реального времени и выводить информацию в удобном виде.

Перехват и запись IP-трафика

в режиме реального времени.

Контроль сетевых каналов

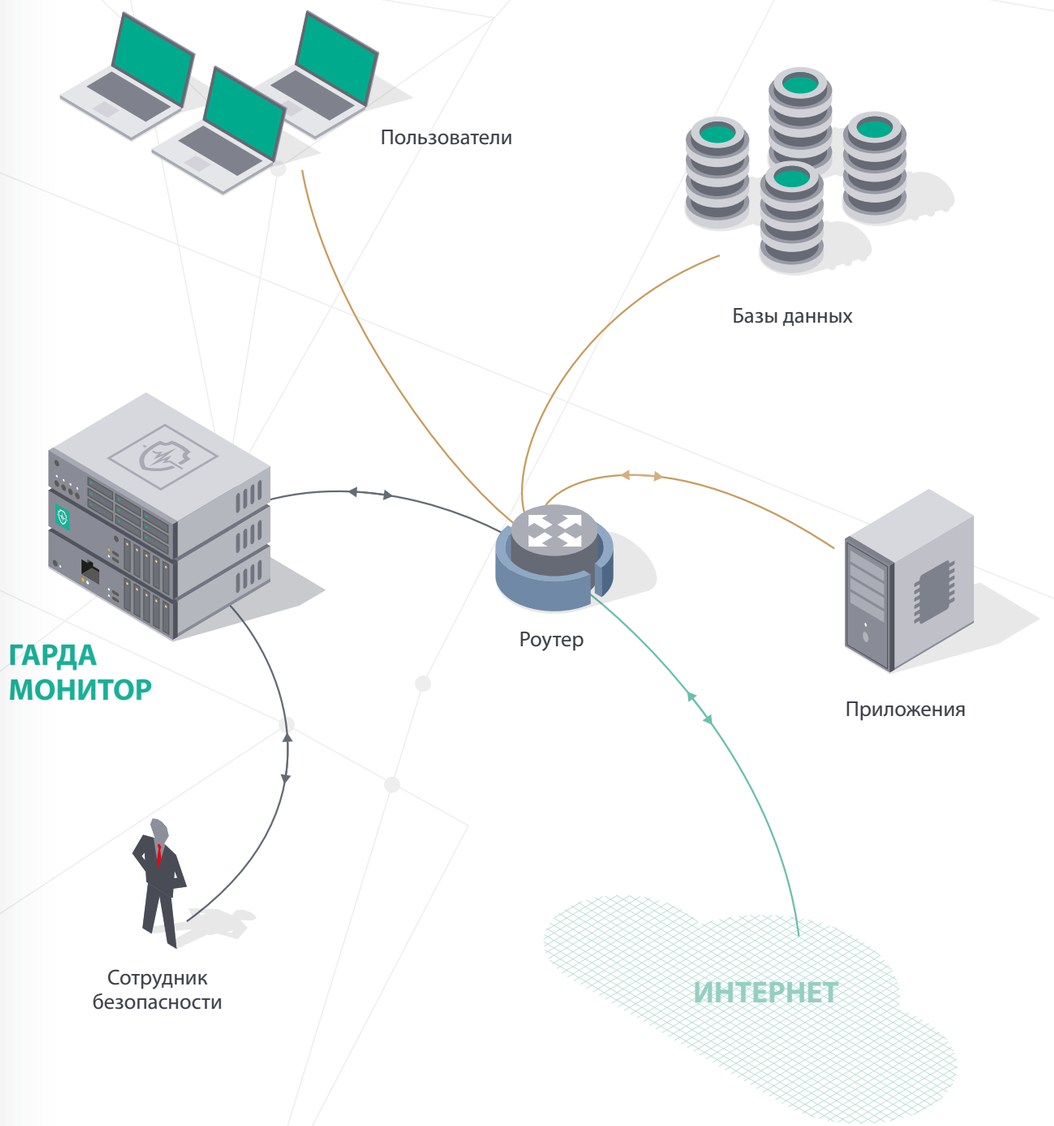
на соответствие передаваемых потоков данных политикам информационной безопасности, включая возможность анализа текстовой информации.

Оптимизированное хранение,

индексация и быстрый поиск по всему объему поступающих данных благодаря высокопроизводительной системе хранения Data Warehouse (DWH) собственной разработки МФИ Софт.

Удобный веб-интерфейс

Многоуровневые отчеты и настраиваемый рабочий экран для удобного управления и анализа задач пользователя.



Функциональные возможности

Выявление аномалий в трафике: всплески или падение сетевой активности, использование нестандартных портов, протоколов, приложений.

Определение географического положения источника и получателя данных, запись метаданных.

Сохранение потоков в «сыром» исходном виде для повторного воспроизведения трафика в лаборатории информационной безопасности.

Полнотекстовый поиск по перехваченным данным и реконструкция объектов по следующим критериям:

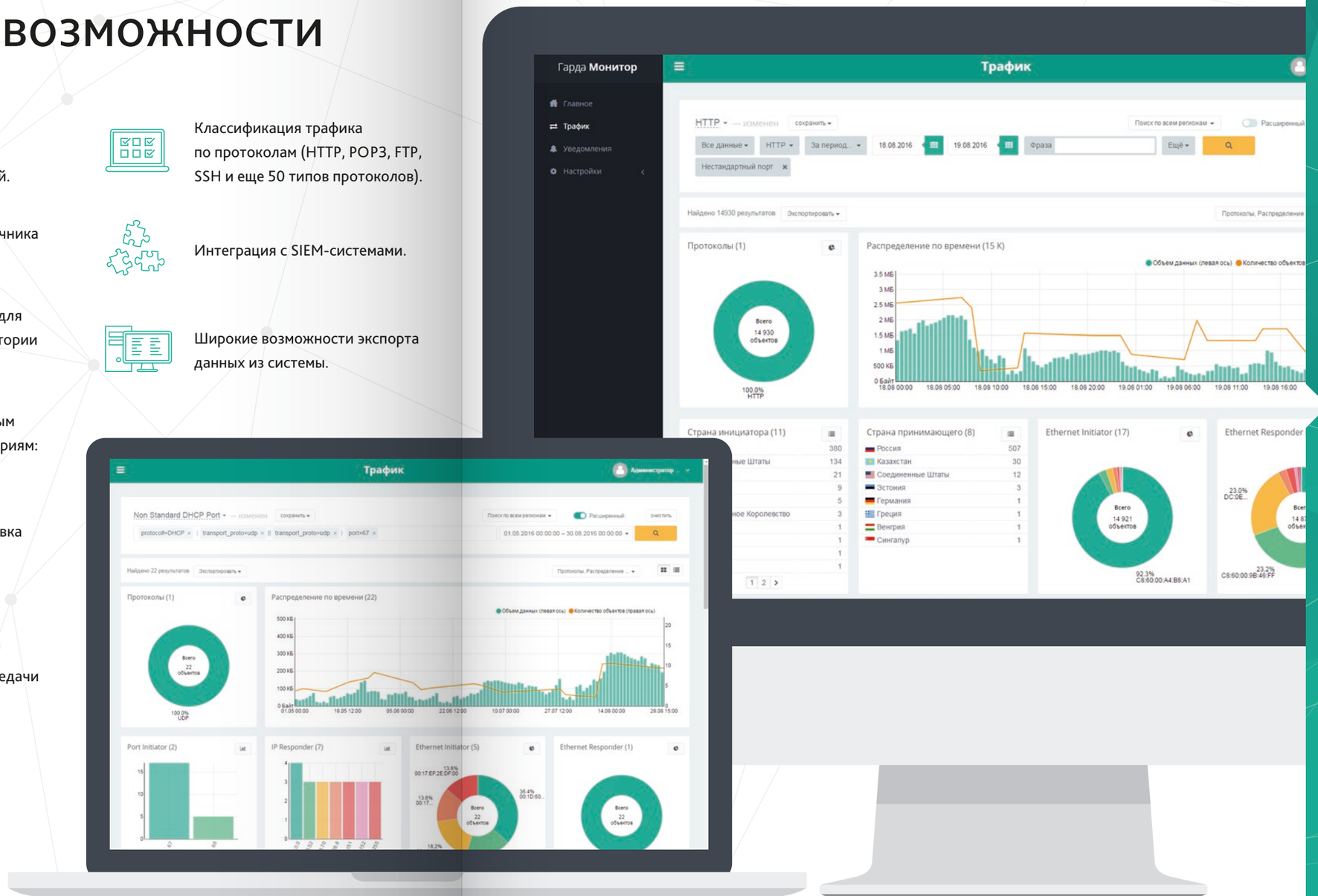
- по MAC-адресам источника и получателя;
- по Vlan ID;
- по версии протокола IP (поле Version заголовка IPv4 или IPv6);
- по IP-адресам источника и получателя;
- по портам источника и получателя;
- по типу протокола транспортного уровня;
- по типу прикладного протокола;
- по полям протоколов HTTP, протоколов передачи почтовых сообщений, сообщений IM и др.;
- по длине пакетов.

Поддержка распределенной инфраструктуры.

Классификация трафика по протоколам (HTTP, POP3, FTP, SSH и еще 50 типов протоколов).

Интеграция с SIEM-системами.

Широкие возможности экспорта данных из системы.



Гарда Монитор. Преимущества

Высокая производительность: анализ трафика со скоростью 10 Гбит/с на модуль, хранение более 100 Тб данных.

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

Библиотека предустановленных политик для выявления инцидентов и возможность настроить свои политики для оперативного контроля трафика в режиме реального времени.

Гибкая система фильтров — мгновенный критериальный поиск, включая детектирование шифрованного трафика.

Предустановленные политики безопасности – оперативное оповещение об инцидентах по заданным критериям.

Фоновый режим работы: система незаметна для привилегированных пользователей и не может быть удалена сотрудником.

Распределённая архитектура – мониторинг трафика всех филиалов компании из единого центра.

Оперативное оповещение о нарушении политик безопасности.

Интерактивные отчеты и понятная аналитика входящего и исходящего трафика, статистика инцидентов.

Не требует сторонних лицензий.

О компании МФИ Софт

МФИ Софт — российская инновационная компания, разработчик систем информационной безопасности, фильтрации интернет-трафика, защиты баз данных, антифрод-решений и систем легального контроля.

«МФИ Софт» осуществляет комплексную поддержку компании-клиента на всех этапах сотрудничества:

Разработка технического решения, инсталляция комплекса

Разработка и адаптация системы под индивидуальные потребности бизнеса

Обучение персонала

Послегарантийное обслуживание

Техническая поддержка

Развертывание занимает от нескольких дней до недели в зависимости от масштабов компании.

Хотите посмотреть систему Гарда Монитор в действии?
Оставляйте заявку, и мы пришлем Вам персональное приглашение на демонстрацию.

ГАРДА
МОНИТОР

МФИ СОФТ

Свяжитесь с нами, чтобы посмотреть систему Гарда Монитор 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 МОНИТОР

Выявление и расследование сетевых инцидентов