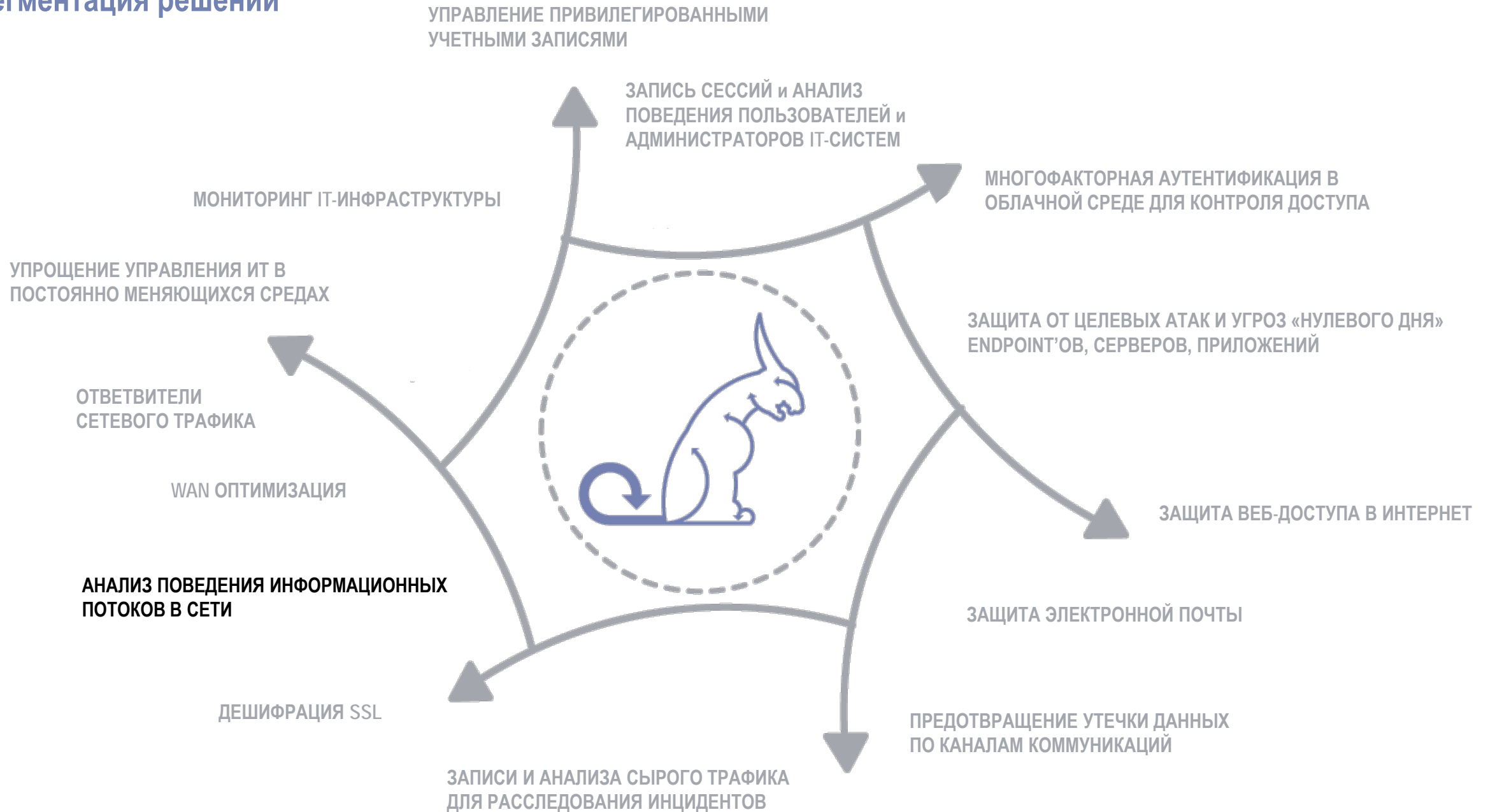


Сегментация решений





Решение Flowmon

АНАЛИЗ ПОВЕДЕНИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ В СЕТИ

<https://www.flowmon.com/en/products/flowmon>

Решение предназначено для мониторинга IP сетей любого масштаба (LAN, WLAN, WAN).

FlowMon предоставляет возможности для анализа информационных потоков в распределенной физической и виртуальной ИТ инфраструктуре с функциональной (по группам пользователей, типам серверов) и географической разбивкой хостов, демонстрацией ключевых количественных и качественных характеристик приложений и возможностью последующего анализа до отдельных пользовательских сессий.

Система относится к классу решений NBA (Network Behavior Analysis – анализ поведения информационных потоков), а также позволяет автоматически выявлять потенциально вредоносное поведение сетевых узлов (сканирование, флуд, попытки «переполнения буфера», односторонняя передача больших объемов данных, долгоживущие соединения с внешними ресурсами и т.д.).

Основной функционал позволяет:

- Накопление, индексация и хранение статистики сетевого взаимодействия всех элементов ИТ инфраструктуры (в физической и виртуальной средах), генерация отчетов на основе этой статистики (в том числе за продолжительные периоды времени). Возможность хранения трафика в виде файла PCAP;
- Наличие собственных коллекторов сбора событий без ограничений по Netflow источникам;
- Поддержка интеграции с Active Directory;
- Максимальная скорость потоков в секунду до 250 000 (на единицу оборудования) с возможностью масштабирования;
- Наличие оптических портов (10/40/100 Гбит/с);
- Производительность сенсоров до 149 000 000 пак/с (на 100Гбит/с) на FPGA платах собственной разработки;
- Наличие механизмов реагирования на инциденты (e-mail, Syslog, SNMP, перенаправление и очистка трафика);
- Возможность аудита конфигураций сетевых устройств (межсетевых экраны и т.д.);
- Автоматическое выявление изменений профилей сетевого поведения рабочих станций и серверов;
- Детектирование аномалий, в том числе внутри VoIP (SIP) трафика;
- Обработка NetFlow (v5, v9), CFlow, JFlow, NetStream, Packeteer-2, Cisco NSEL, Cisco HSL и IPFIX, Syslog, SNMP, NBAR;
- Возможность соотнесение адресов в NAT сессиях;
- Наличие функции автопоиска нового оборудования в сети;
- Устранение дублирования сетевой статистики при одновременном сборе ее с большого количества источников;
- Анализ производительности работы сети и приложений (RTT, SRT, jitter, delay);
- Анализ уровня качества веб-сервисов;
- Построение отчетов по объемам переданных данных за длительный период с целью выявления тенденций роста ИТ инфраструктуры и планирования ее развития;
- Наличие API для интеграции со смежными системами;
- система поддерживает гибкий функционал построения отчетов по безопасности и производительности сетей.

Стоимость решения формируется из следующих составляющих:
устройства и модули

Преимущества:

- ✓ Оперативно обнаружит проблемы в сети, что ускорит время их устранения.
- ✓ Кроме анализа пропускной способности сети и ее оптимизации, также определит атаки (Сканирование, DDoS, Интернет-червей, взлом).
- ✓ Идентификация пользователя даёт возможность видеть его активность в сети и выводить отчёты на основании этой информации.

Решение состоит из самостоятельных модулей:

1. Probe – сбор и обработка трафика
2. Collector – накопление статистики
3. ADS – обнаружение аномалий в трафике
4. DDoS Defender – определение атак
5. APM – мониторинг производительности приложений
6. Traffic Recorder - запись сетевых пакетов

Технические возможности

- Автоматическое выявление потенциально вредоносного поведения сетевых узлов (сканирование, флуд, попытки «переполнения буфера», односторонняя передача больших объемов данных, долгоживущие соединения с внешними ресурсами и т.д.);
- Выявление нового вредоносного ПО, для которого не существует антивирусных сигнатур (противодействие атакам нулевого дня);
- Противодействие потенциальным утечкам информации (инсайдеры);
- Автоматическое выявление векторов распространения вредоносного ПО (сетевые черви);
- Автоматическое выявление взаимодействия внутренних сетевых узлов с botnet-сетями;
- Автоматическое выявление наиболее подозрительных узлов сети;
- Автоматическое выявление узлов сети, наиболее подверженных атакам;
- Автоматическое выявление узлов сети, передающих/получающих большой объем данных;
- Автоматическое определение нового оборудования в контролируемой сети;
- Автоматическое определение пиринговых сетей, в том числе клиентов BitTorrent, Gnutella;
- Автоматическое обнаружение широковещательных штормов.

