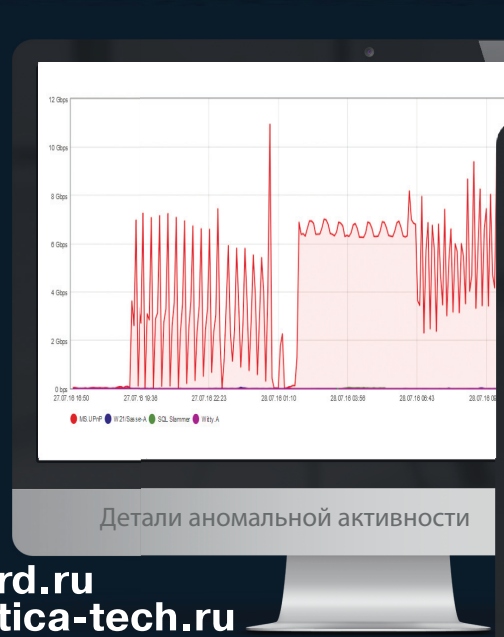
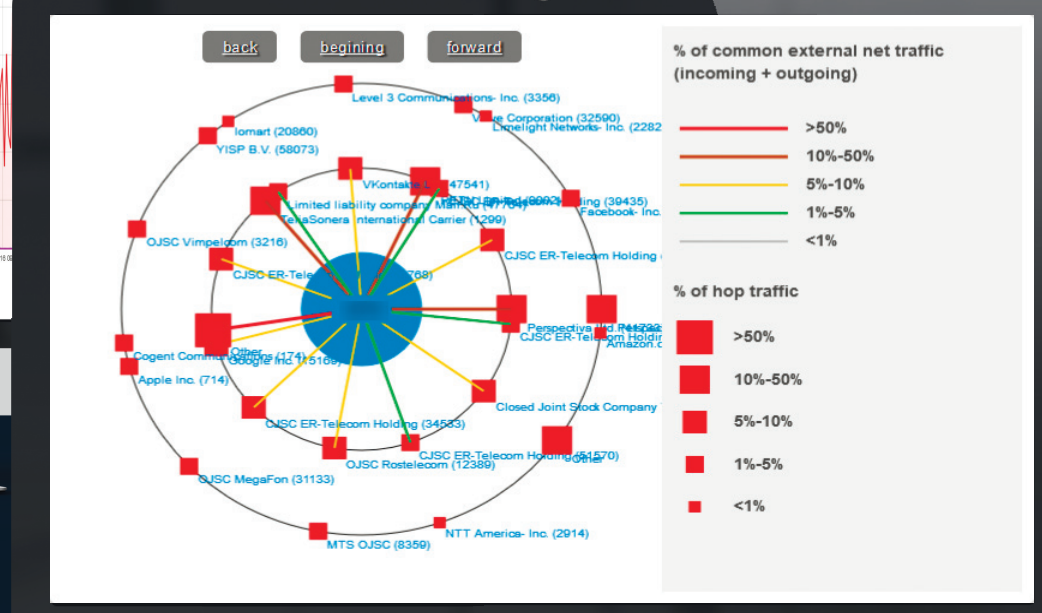
invGUARD

Система защиты от сетевых атак

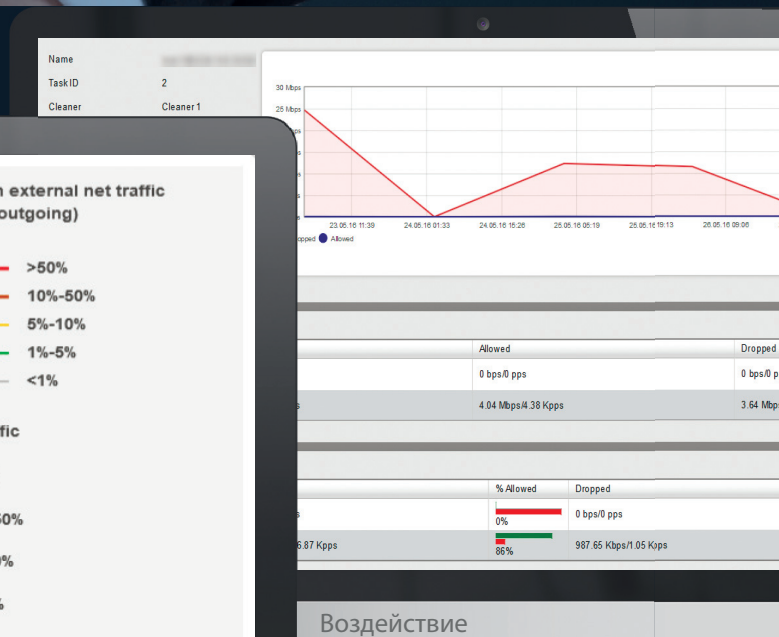
INOVENTICA TECHNOLOGIES



Детали аномальной активности



BGP пиры



Воздействие инфицированных хостов

invguard.ru
inoventica-tech.ru

facebook.com/inoventicagroup

twitter.com/Inoventica

vk.com/inoventica

www.linkedin.com/company/inoventica-services

instagram.com/inoventica

INOVENTICA TECHNOLOGIES

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА invGUARD

- Лучшее на рынке соотношение «цена/функциональность»
- Возможна работа анализатора в среде виртуальной машины
- Возможность применения invGUARD как дополняющего решения в сети (заполнюнность внедрения, не требует модернизации или замены имеющейся ИКТ-инфраструктуры)
- Сохранение при внедрении invGUARD ранее сделанных инвестиций в ИКТ-инфраструктуру
- Автоматическое детектирование и подавление атак
- Программный интерфейс invGUARD API для управления системой
- Встроенные возможности подключения к автоматической системе управления виртуализацией loSphere
- Более 100 шаблонов детектирования и подавления атак
- Простая кастомизация по требованиям заказчика
- Возможность создания для конечного потребителя привлекательных по цене/бесплатных услуг по защите от DDoS-атак
- Возможность управления invGUARD с доступом через мобильные устройства
- 24/7 поддержка системы, включая возможность on-site поддержки

ВАРИАНТЫ ПРИОБРЕТЕНИЯ СИСТЕМЫ invGUARD

Разовый платёж

Ежемесячные платежи

Разделение доходов за фактически оказанные конечному пользователю услуги по защите от кибератак

Возможность приобретения, как всей системы, так и её отдельных подсистем (invGUARD AS, invGUARD AS & invGUARD CS)

5+ Тбит/с	скорость анализа трафика и подавление атак в сети
100+	маршрутизаторов в едином интерфейсе управления
20000+	наблюдаемых объектов (информационные системы, сайты, интернет-магазины и др.)
Мультивендорность	сетевое оборудование: Juniper, HPE, H3C, Cisco, Huawei, Alcatel, Extreme
250+	типов отчетов по различным видам трафика и объектов
100+	видов детектируемых атак
10000+	детектируемых угроз в сутки
80-	часов на внедрение системы

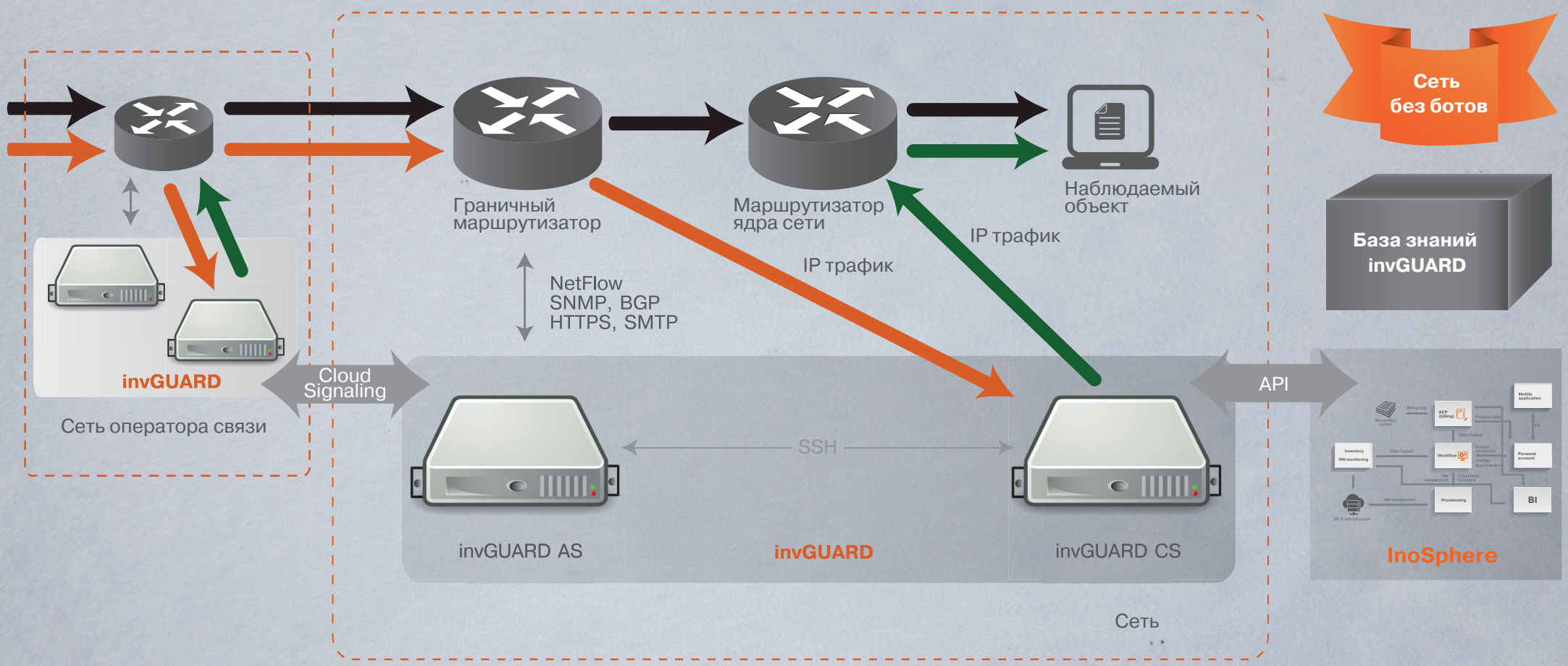
ОБЛАСТЬ ПРИМЕНЕНИЯ invGUARD

- телеком операторы
- сервис-провайдеры
- операторы центров обработки данных
- медиа-компании (СМИ, интернет-СМИ)
- банки и финансовые организации
- компании с развитой внутренней ИКТ-инфраструктурой
- хостинговые компании

ЦЕЛИ ВНЕДРЕНИЯ invGUARD

1. Решение, эффективное по затратам, для детектирования и предотвращения кибератак (DoS/DDoS-атак и воздействий, не имеющих четко выраженных сигнатур)
2. Снижение рисков от воздействий атак на отказ в обслуживании наблюдаемых (защищаемых) объектов, таких как веб-сайты, интернет-магазины, медиа-порталы и других
3. Удобный инструмент для анализа трафика и оптимизации сетевой инфраструктуры
4. Простая интеграция с существующими системами мониторинга и платформами управления сетями по протоколу SNMP (HP OV, IBM Tivoli, Zabbix, Nagios и другие)
5. Эшелонированная защита от сетевых атак для повышенного уровня безопасности (Cloud Signaling)
6. Мониторинг исполнения SLA по доступу к информационным ресурсам
7. Эффективный инструмент для управления затратами на услуги связи
8. Дополнительный источник выручки по услугам защиты от DoS/DDoS-атак для B2B/B2C клиентов (простая интеграция с платформой управления облачными услугами InoSphere)

АРХИТЕКТУРА СИСТЕМЫ invGUARD



Наименование	Назначение	Применяемые технологии
invGUARD AS - анализ трафика до 1 Тбит/сек - обработка до 100 тысяч flow/сек	- Анализ трафика и состояния сети - Детектирование и подавление атак - Управление системами invGUARD CS/CS-01 - Функционал Cloud Signaling для построения эшелонированной защиты - Личный кабинет пользователя (клиента) - Централизованный мониторинг сетевого оборудования - Настраиваемая автоматическая защита от кибератак	Анализ трафика в сети: NetFlow v5, v9 and IPFIX Опрос маршрутизаторов: SNMP v2c и v3 Управление маршрутизацией: BGP v4 Интеграция с системами мониторинга Уведомление пользователей invGUARD API
invGUARD CS - фильтрация (очистка) трафика до 20 Гбит/сек, 30 млн пакетов/сек	- Очистка трафика от нелегитимной активности - Фильтрация трафика по различным типам DDoS-атак	Высокоскоростная фильтрация (очистка) трафика с использованием специальных сетевых плат
invGUARD CS–01 - фильтрация (очистка) трафика до 1 Гбит/сек, 3 млн пакетов/сек	- Очистка трафика от нелегитимной активности - Фильтрация трафика по различным типам DDoS-атак	Фильтрация (очистка) трафика с использованием сетевых плат с поддержкой intel DPDK