Lancope®

Новое поколение систем сетевой безопасности: Повышение защищенности с использованием инструментов анализа информационных потоков (Network Flow)

Андрей Акинин
Директор по развитию бизнеса
Web Control

С чем мы боремся?

Lancope
Network Performance + Security Monitoring

- **Вторжение** - Попытка или факт нарушения конфиденциальности, целостности, доступности или обхода систем безопасности компьютерных систем и сетей (неправомочный доступ).

- Вторжение может быть обусловлено:

- Не смотря на то что вторжения опасны по определению, многие из них не причиняют вреда.
- Нередко они обусловлены ошибками пользователей или неправильными настройками.

Типовые угрозы

Lancope
Network Performance + Security Monitoring

- Утечка информации
- Повреждение инфраструктуры
- Потеря репутации
- Деградация уровня сервиса
- Нарушенияе функционирования, злоумышленное или неправомочное использование систем
- Нарушение требований закона

Как Вы защищаете Вашу сеть?

Lancope
Network Performance + Security Monitoring

- Antivirus? Firewall? Url фильтр? IDS/IPS? Antispam фильтр? Что то еще?

  Чем это отличается от face-control в популярном баре?...

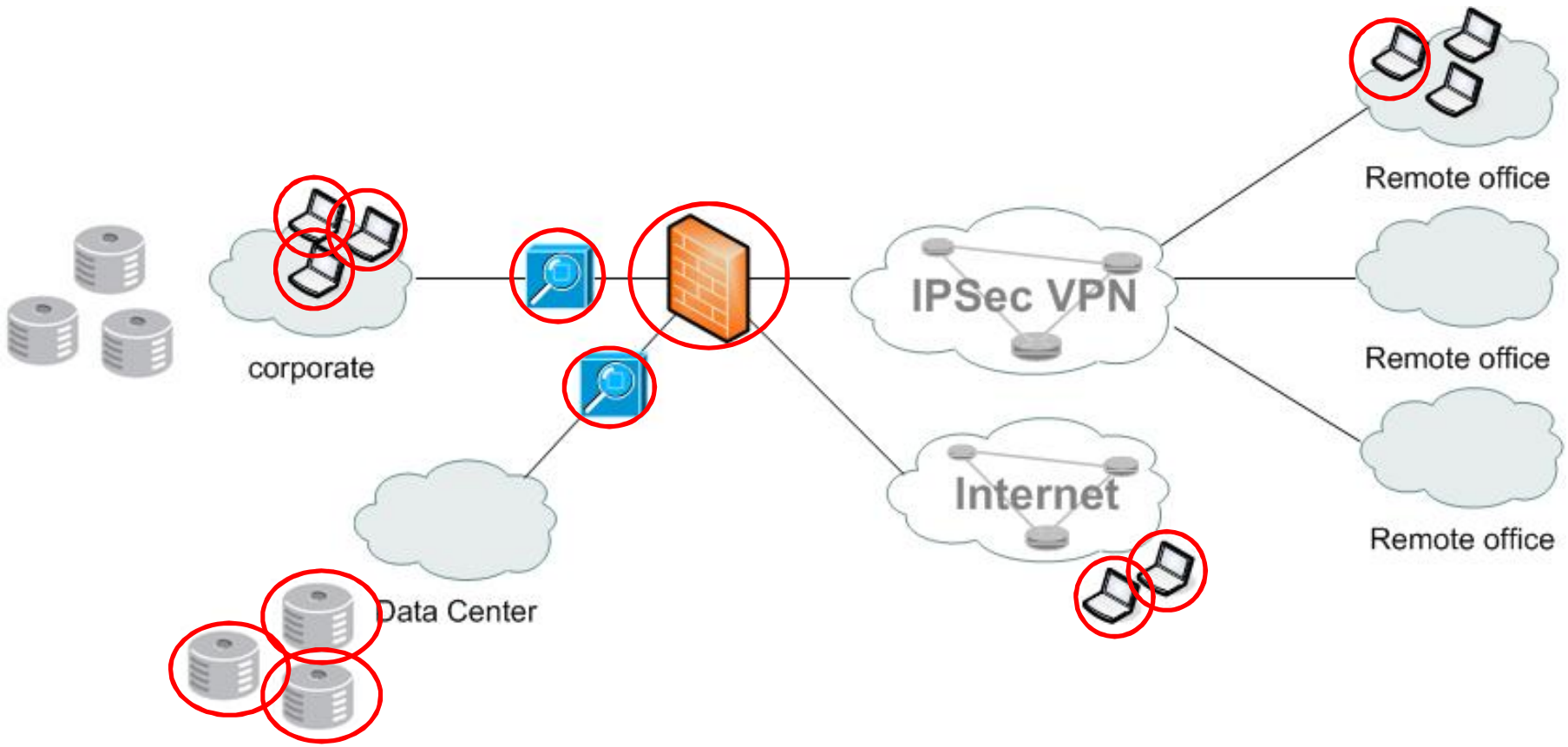
  Это надежно?

- Широко применяемые методы защиты узлов и сетей существуют более 25 лет.
- Каждый год средства защиты становятся «быстрее, умнее, лучше» ….

  но они по сути те же что и 25 лет назад

Традиционный подход

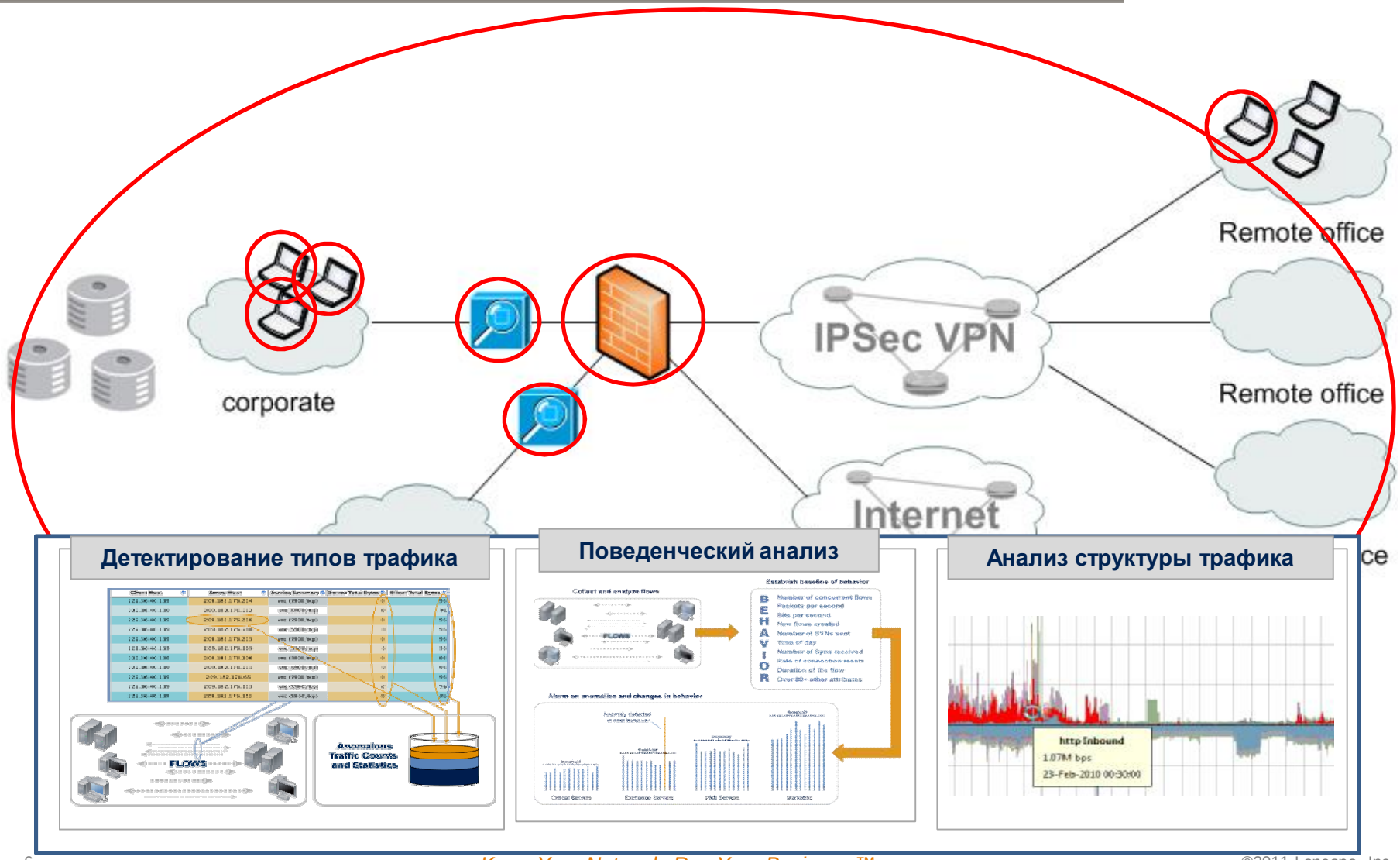
Lancope
Network Performance + Security Monitoring



Know Your Network. Run Your Business.™

Новый подход

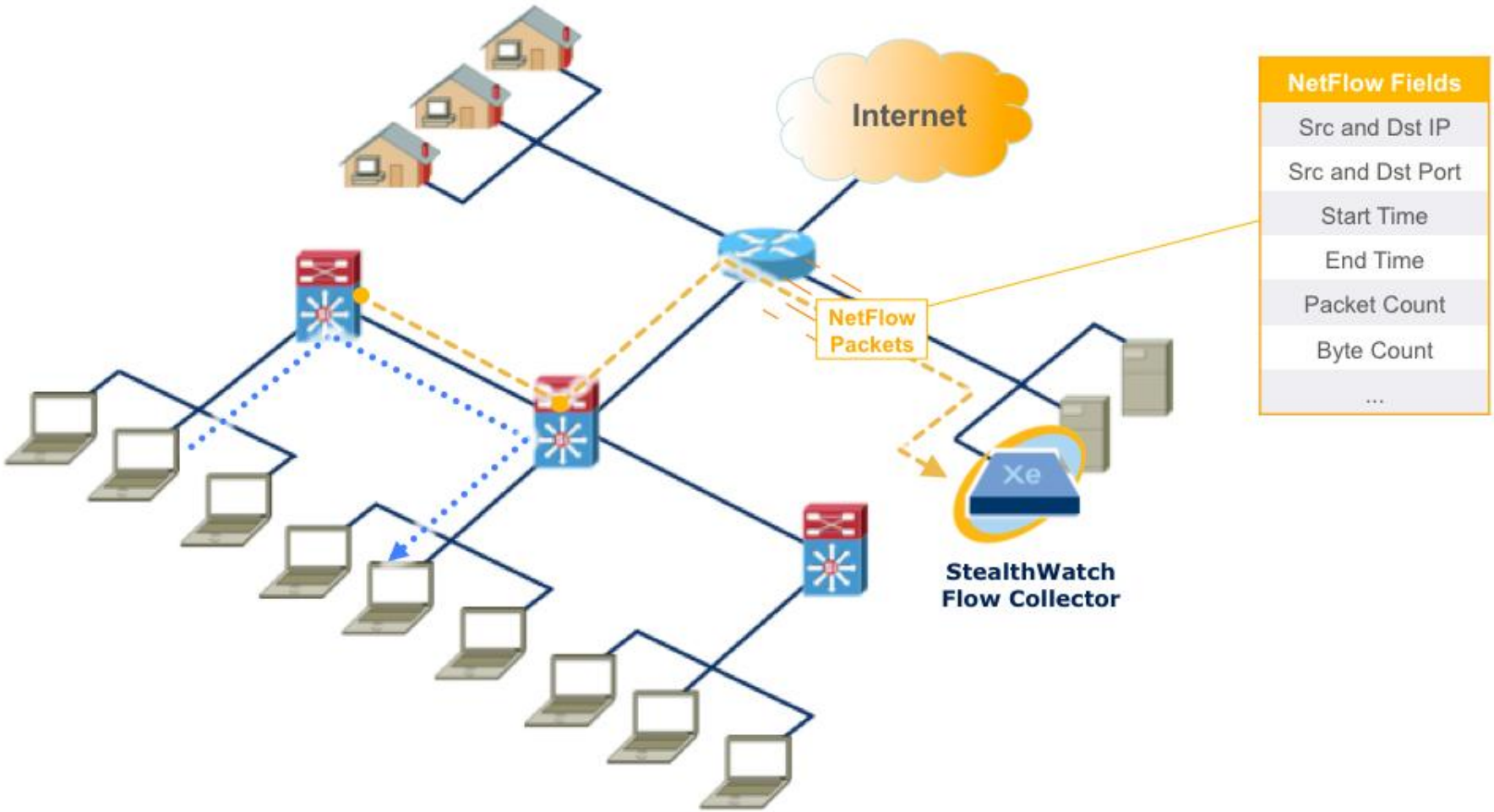
Lancope
Network Performance + Security Monitoring



Know Your Network. Run Your Business.™

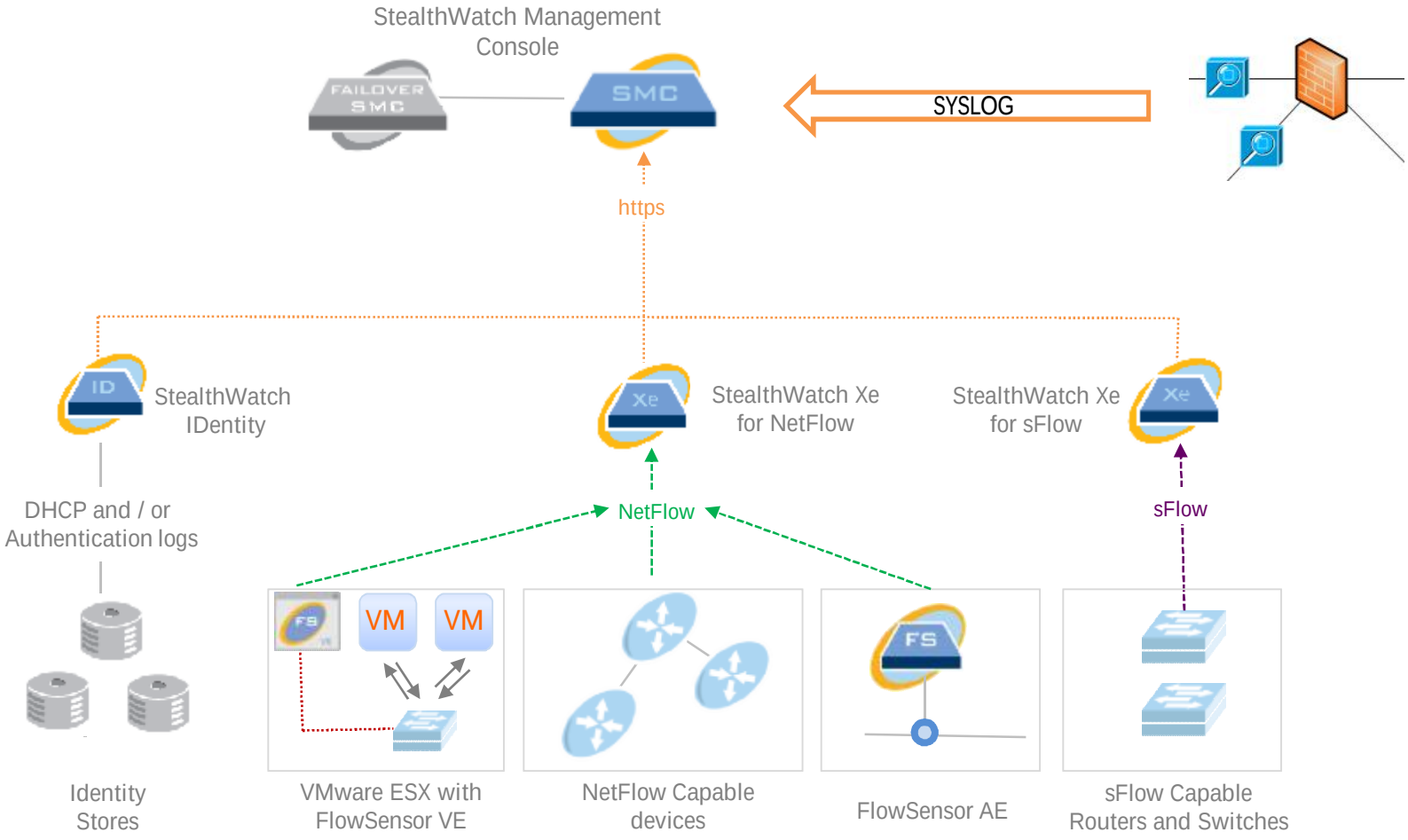
Как получить первичные данные?

Lancope
Network Performance + Security Monitoring



Know Your Network. Run Your Business.™

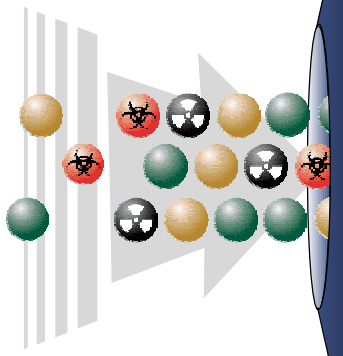
Решение StealthWatch



Know Your Network. Run Your Business.™

Преимущества анализа потоков

Lancope
Network Performance + Security Monitoring



FLOW ANALYSIS

Обнаружение вторжения

- Ø Быстрое обнаружение новых типов атак
- Ø Сдерживание атаки и минимизация ущерба
- Ø Обнаружение внешних и внутренних угроз

Визуализация и корреляция

- Ø Контроль сети и безопасности
- Ø Точная идентификация и приоретизация угроз
- Ø Не только сетевое оборудование, но и хосты

Применение политик

- Ø Обнаружение не авторизованных приложений
- Ø Изоляция подозрительного трафика
- Ø Применение политик

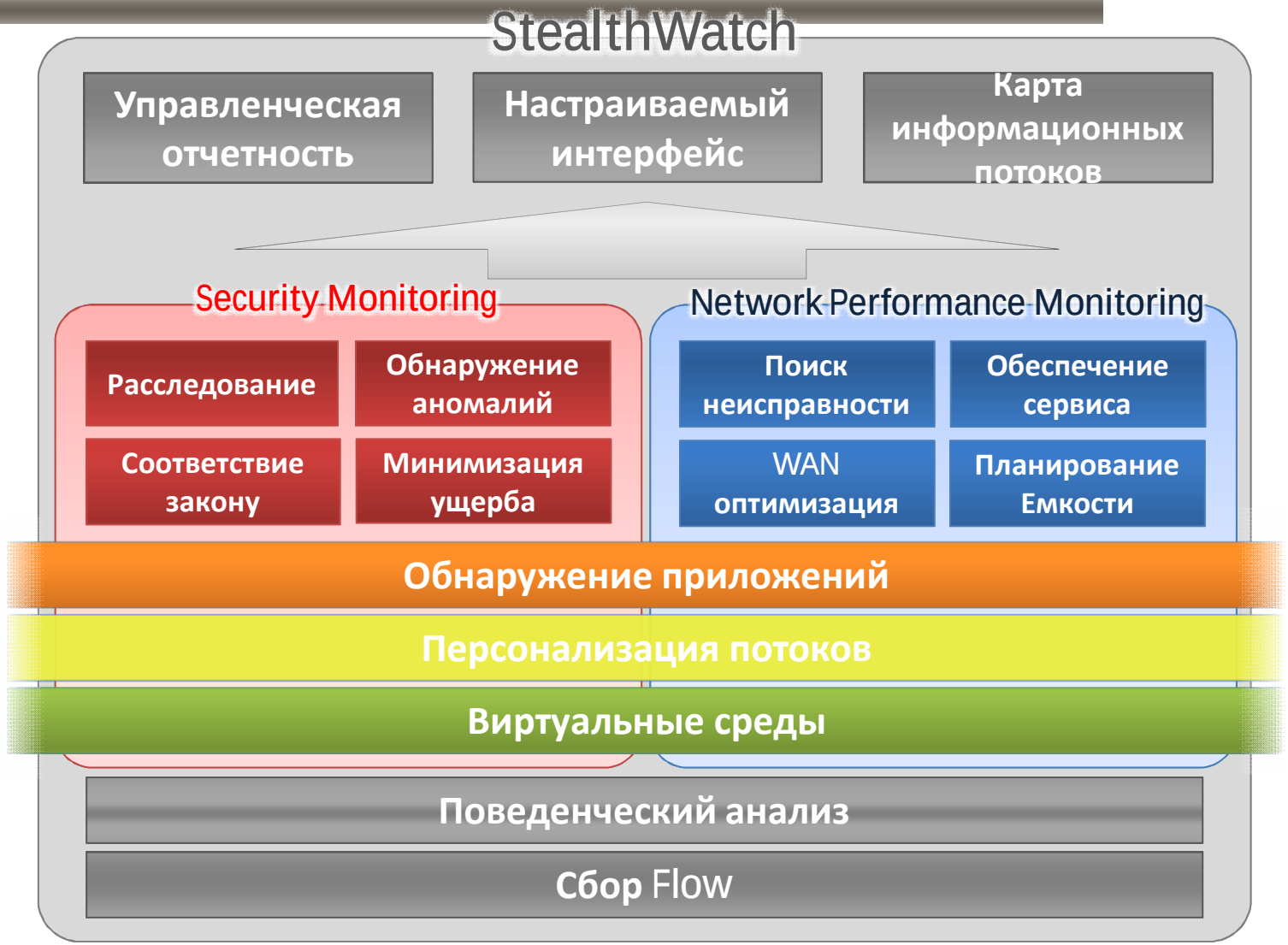
Протокол и расследование

- Ø Выявление первопричины и затронутых хостов
- Ø Ускорение исправления
- Ø Детальный анализ атак

Анализ трафика

- Ø Анализ тренда и планирование емкости
- Ø Тест Firewall и планирование
- Ø Мониторинг производительности сети

StealthWatch улучшенный анализ потоков



Know Your Network. Run Your Business.™

Что мы имеем?

Lancope
Network Performance + Security Monitoring

- Традиционные методики – необходимый базис

Но:

- Ищут известные угрозы
- Дают обобщенную информацию об инциденте

Нужно:

- Понимание реальной ситуации в сети
- Различать «нормальное» и «аномальное»

Анализ потоков:

- В комбинации с традиционными методами дает значительно лучшую защиту
- Новые методы бросают вызов производительности традиционных инструментов безопасности

Спасибо за внимание!

Lancope
Network Performance + Security Monitoring

Приглашаю познакомится с примером
из практики применения в секции III

16:35 – 16:55

Как увеличить безопасность сети, используя традиционную сетевую телеметрию

Андрей Акинин, директор по развитию бизнеса компании Web Control

Заказчик: Telenor

telenor