Телеметрия
для мониторинга сети и контроля информационной безопасности

Andrii Ovrashko
Systems Engineer

18 May 2016

Agenda

- Информационная безопасность современных сетей. Планирование.
- Оценка текущих средств и мер
- Способы обогащения картины ИБ
- **Network as a Sensor**
- Контроль с пониманием деталей
- Добавляем TrustSec = **Network as an Enforcer**
- Собираем архитектуру
- Что полезного можно добавить с SDN подходом?

Cisco Forum

Что нам стоит ИБ в сети построить!

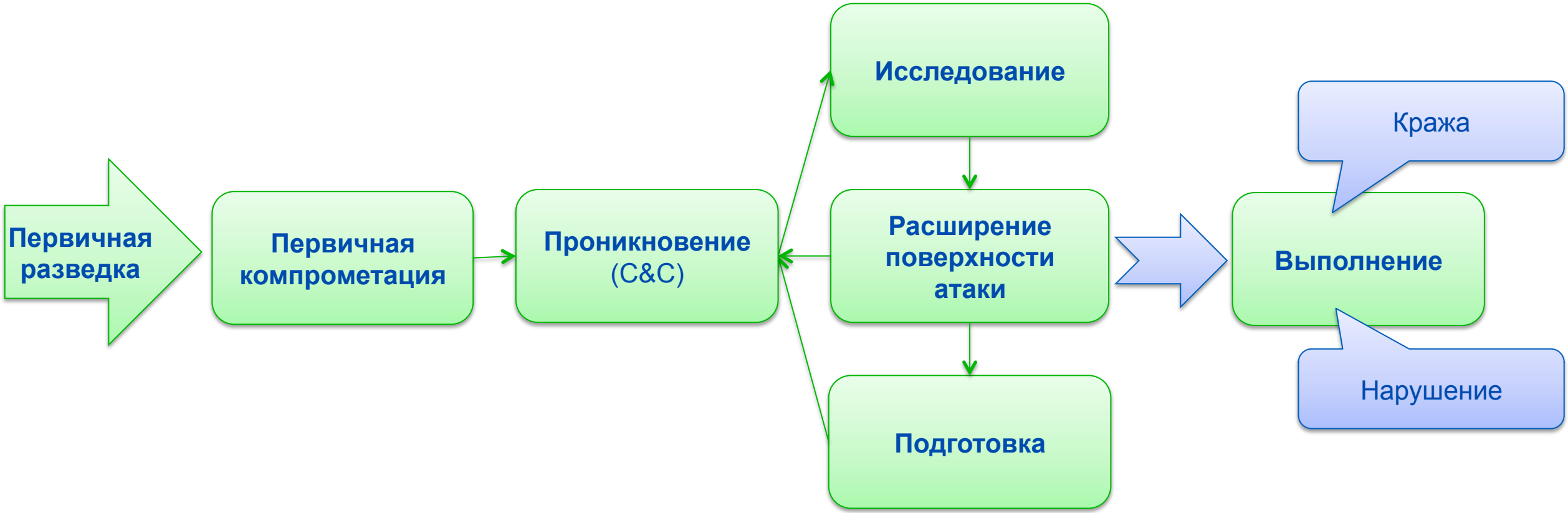
[1 / 7]

We're ready.
Are you?

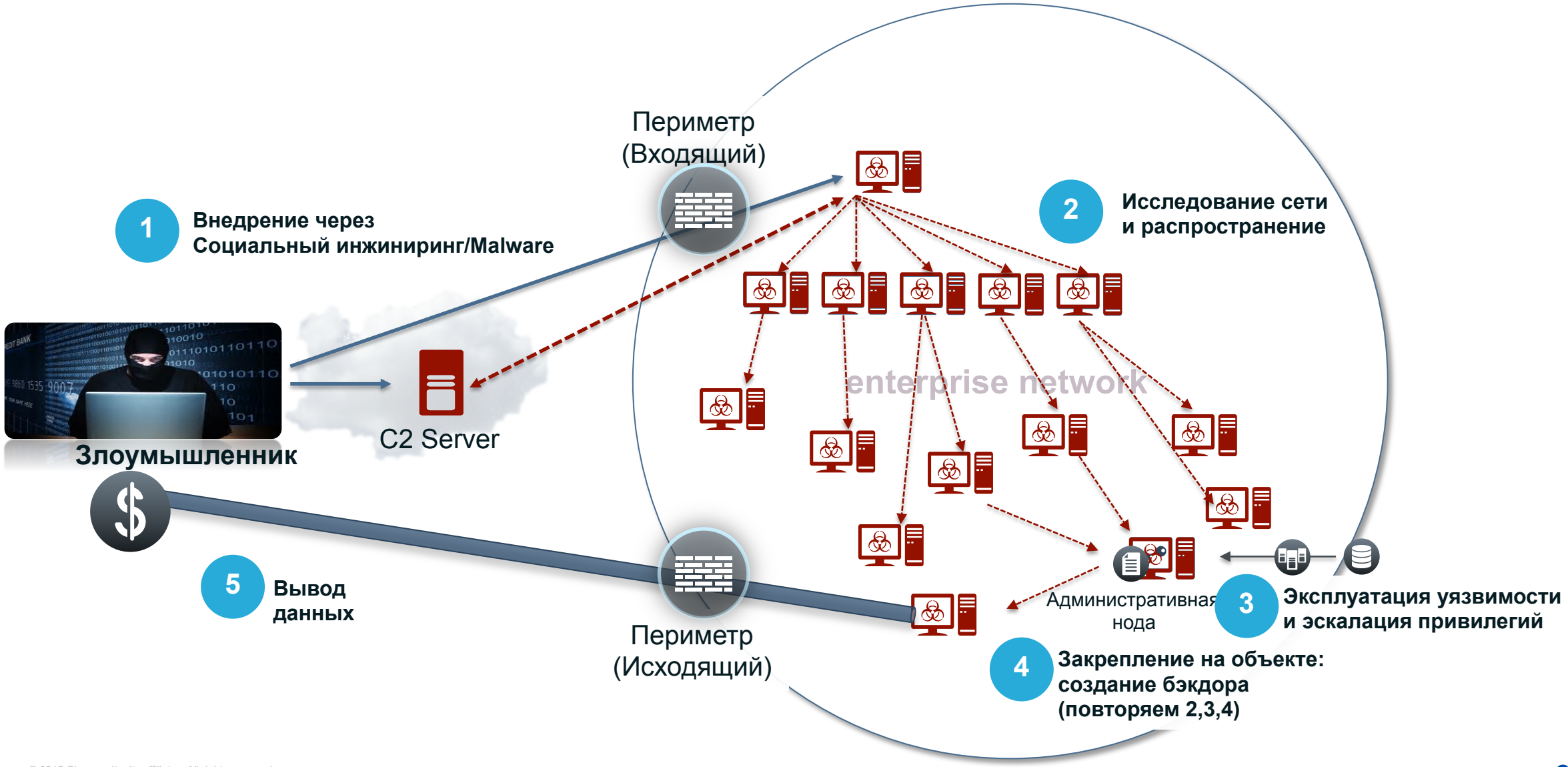
Этапы построения системы защиты предприятия
Планирование

- Модель угроз
- Оценка вероятности реализации угроз ИБ
- Оценка рисков (что может быть принято как оправданный риск)
- Оценка ожидаемых годовых потерь
- Определение классов систем защиты и границ бюджета
- Определения трудовых ресурсов и построение процессов
- Оценка сценария «худший случай»
- Пересмотр и возможные коррективы плана

Из чего состоит жизненный цикл типовой атаки?



Анатомия взлома сети



6

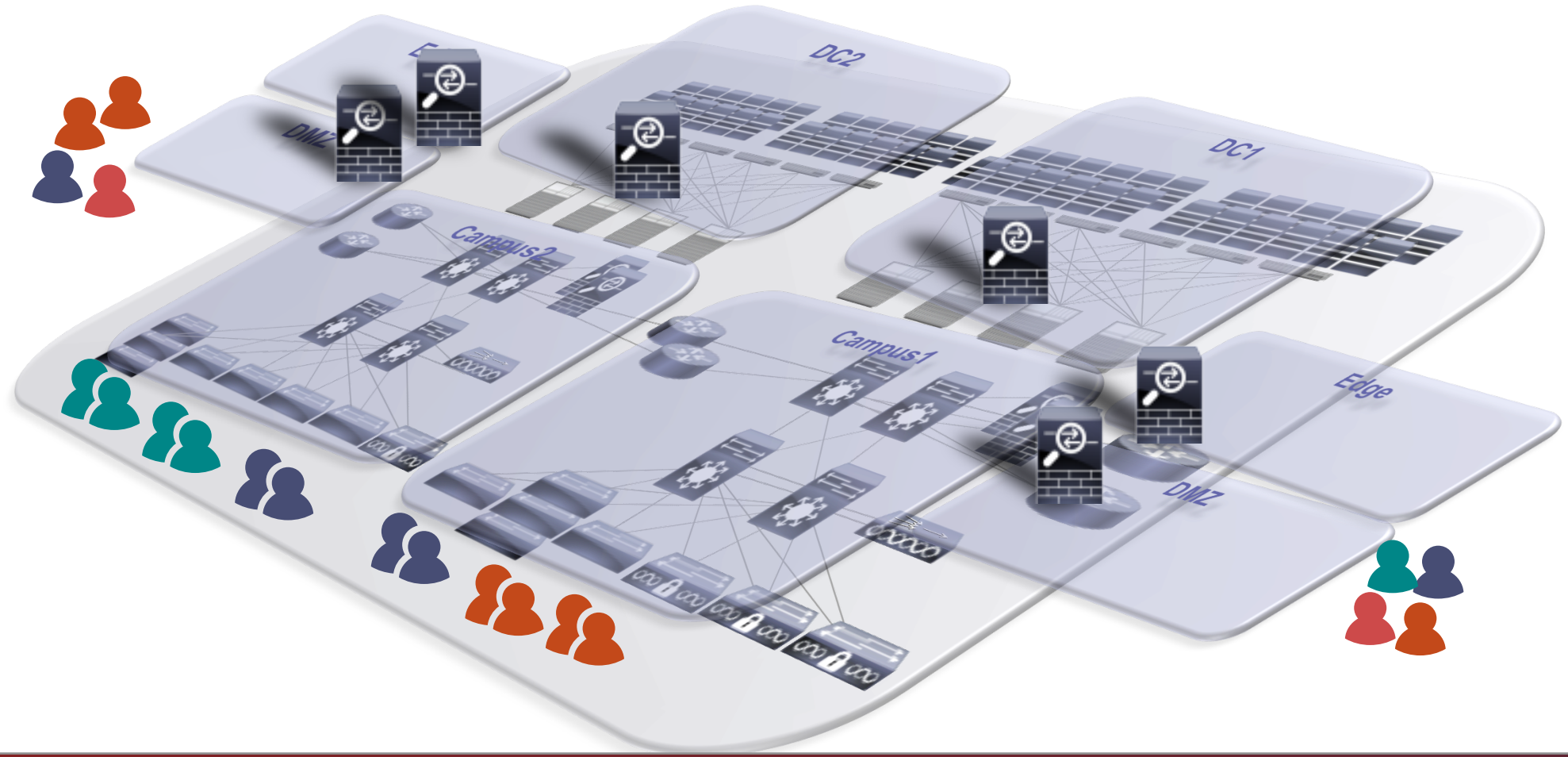
Cisco Forum

Что уже есть в сети из средств ИБ?

[2 / 7]

We're ready.
Are you?

Сетевая безопасность считалась простой



Традиционная сетевая безопасность

Firewalls, IPS, VPN, AAA

Однако это время прошло…

Где периметр?
Где границы сегментов?
Какие средства мониторинга и обеспечения ИБ необходимы?

Мобильность и BYOD

Облако

IoT

Новые бизнес модели
Облака, Мобильность и BYOD, IoT

Традиционная сетевая безопасность
Firewalls, IPS, VPN, AAA

Увеличенные
Площадь атаки
Масштабы действий
Сложность угроз

Семь простых правил

Список первоочередных мер

1. Знать своего врага и понимать методики
2. Иметь полную набюдаемость всей сети
3. Иметь эффективные «инструменты» (прогамные и аппаратные средства)
4. Применять архитектурный подход к инф.безопасности
5. Уделять внимание реальной настройке средств защиты
6. Учитывать статистику поведения сети, анализ трендов угроз и контекст получаемых машинных данных
7. Применять динамические репутационные данные для принятия решений

Как может сеть помочь решить задачи ИБ?

Мобильность и BYOD

Облако

IoT

Сеть как сенсор

Сеть как средство контроля

Новые бизнес модели

Cloud, Mobility & BYOD, IoT

Традиционная сетевая безопасность

Firewalls, IPS, VPN, AAA

+ Основы сетевой безопасности

Роутинг, Свитчинг, Беспроводная сеть

Увеличенные

Площадь атаки

Масштабы действий

Сложность угроз

Cisco Forum

Что можно добавить?

[3 / 7]

We're ready.
Are you?

Телеметрия с сети и серверов

NetFlow

Телеметрия с рабочих мест

AnyConnect v4 [APEX]

SDN способы ответвления трафика … >>>

Nexus Data Broker

>>> … для получения телеметрии и других услуг ИБ

[Q1] Что такое NetFlow?

Cisco Forum

Подробней о NetFlow и концепции Network as a Sensor [NaaS]

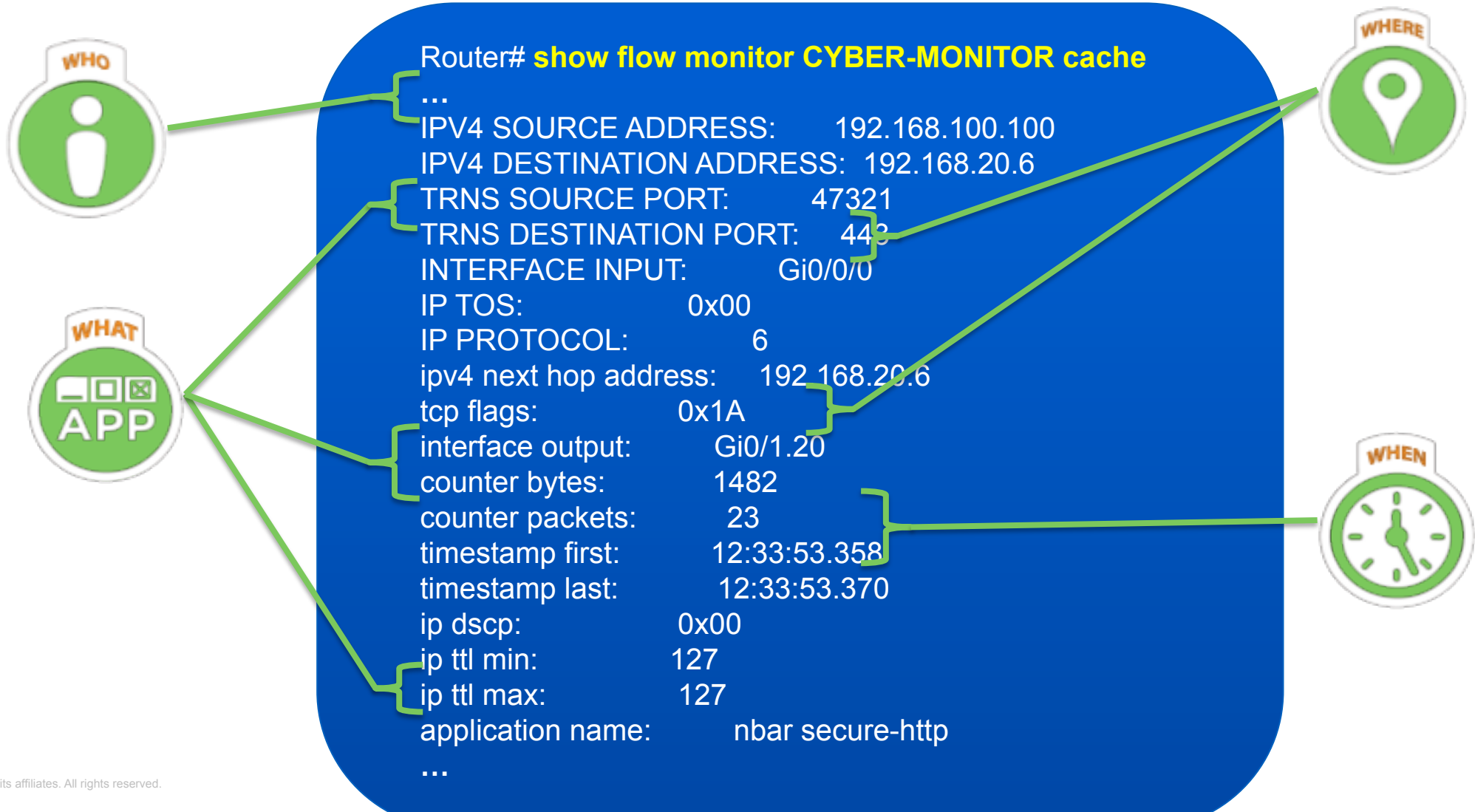
[4 / 7]

We're ready.
Are you?

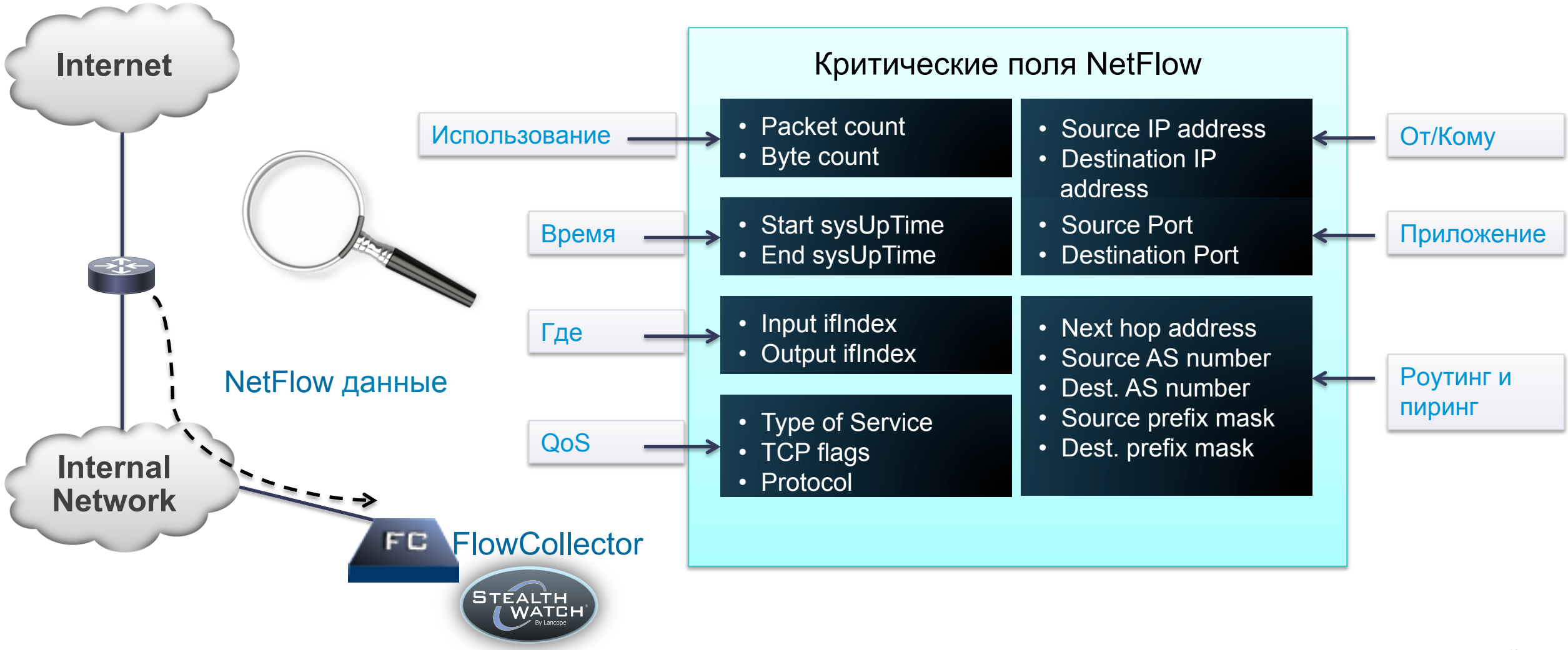
Сеть как сенсор
Анализ Netflow может помочь

NetFlow = Метаданные = Видимость

A single NetFlow Record provides a wealth of information



Контекст и видимость с Netflow



Инфраструктура Cisco

Несемплированных Netflow – ключ к наблюдаемости сети

Sampled = частичный

- Часть трафика, обычно менее 5%,
- Дает быстрый взгляд в сеть
- *Похоже на чтение каждой 20-й страницы книги - технической книги-справочника ☺*

Unsampled = ВЕСЬ

- Весь тафик подлежит сбору
- Предоставляет исчерпывающий обзор всей сетевой активности
- *Эквивалент внимательного постраничного чтения + пометки на полях + закладки*

Семплирование полезно для мониторинга сети, но не для безопасности

Чем сеть может помочь видеть и знать больше?

Сеть как сенсор

Обнаружение Аномальных потоков, Malware

Пример: Связей с подозрительными хостами, Распространение Malware внутри, Утечка данных

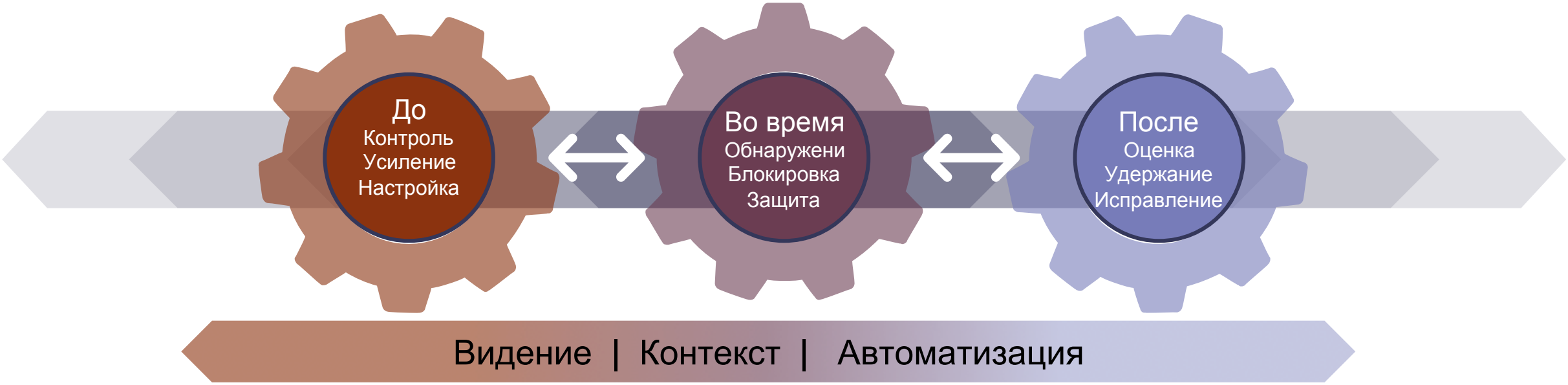
Обнаружение Использования приложений, Нарушение политики доступа пользователем

Пример: Временный сотрудник получает доступ к финансовым данным

Расследование Инцидентов безопасности и усиление защиты = жизненный цикл ИБ

Пример: Временный сотрудник соединяется к неавторизованной точке доступа в филиале

Новая модель безопасности и «Сеть как сенсор»



ДО Усиление	**Во время** Обнаружение	**После** Оценка
Обнаружение и классификация устройств Создание базового профиля Внедрение политики и сегментация	Обнаружение аномального трафика Обнаружение нарушения политики	Идентификация устройств подверженных риску Сбор данных Укрепление защитных мер

[Q2] Ключевые преимущества NetFlow?

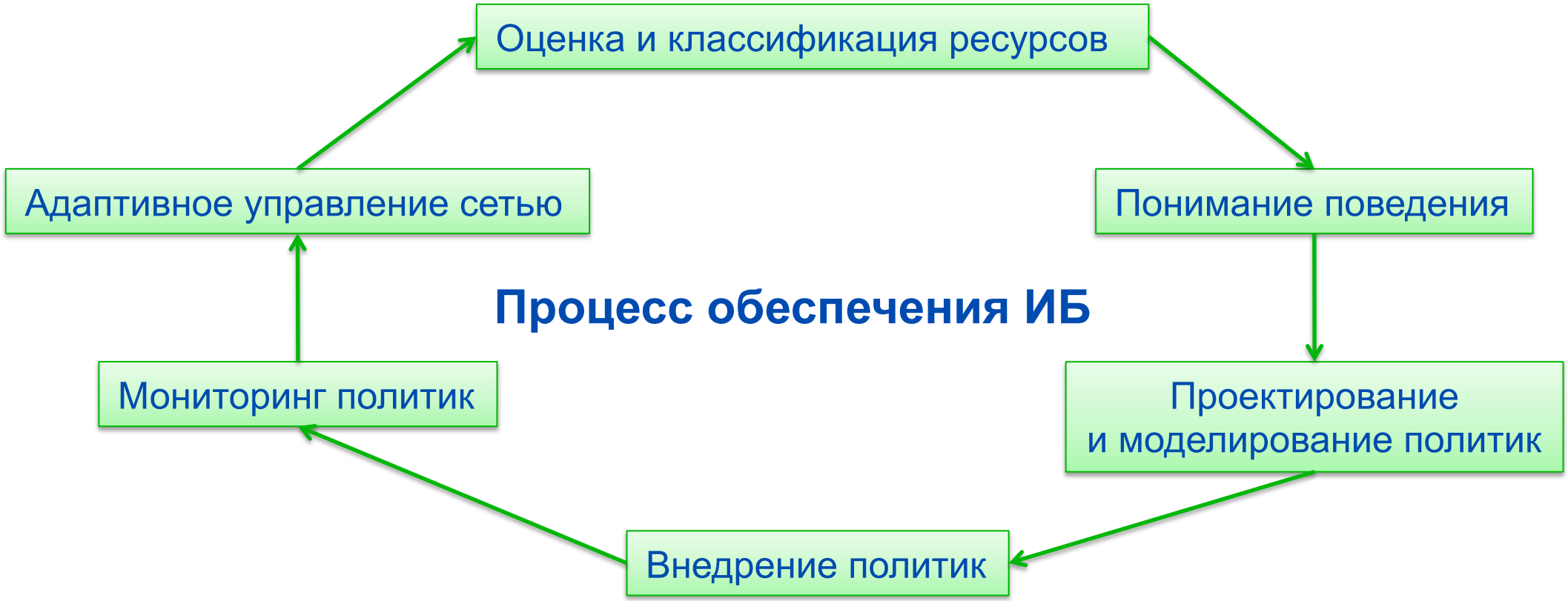
Cisco Forum

Телеметрия для автоматизации реагирования на атаки

[5 / 7]

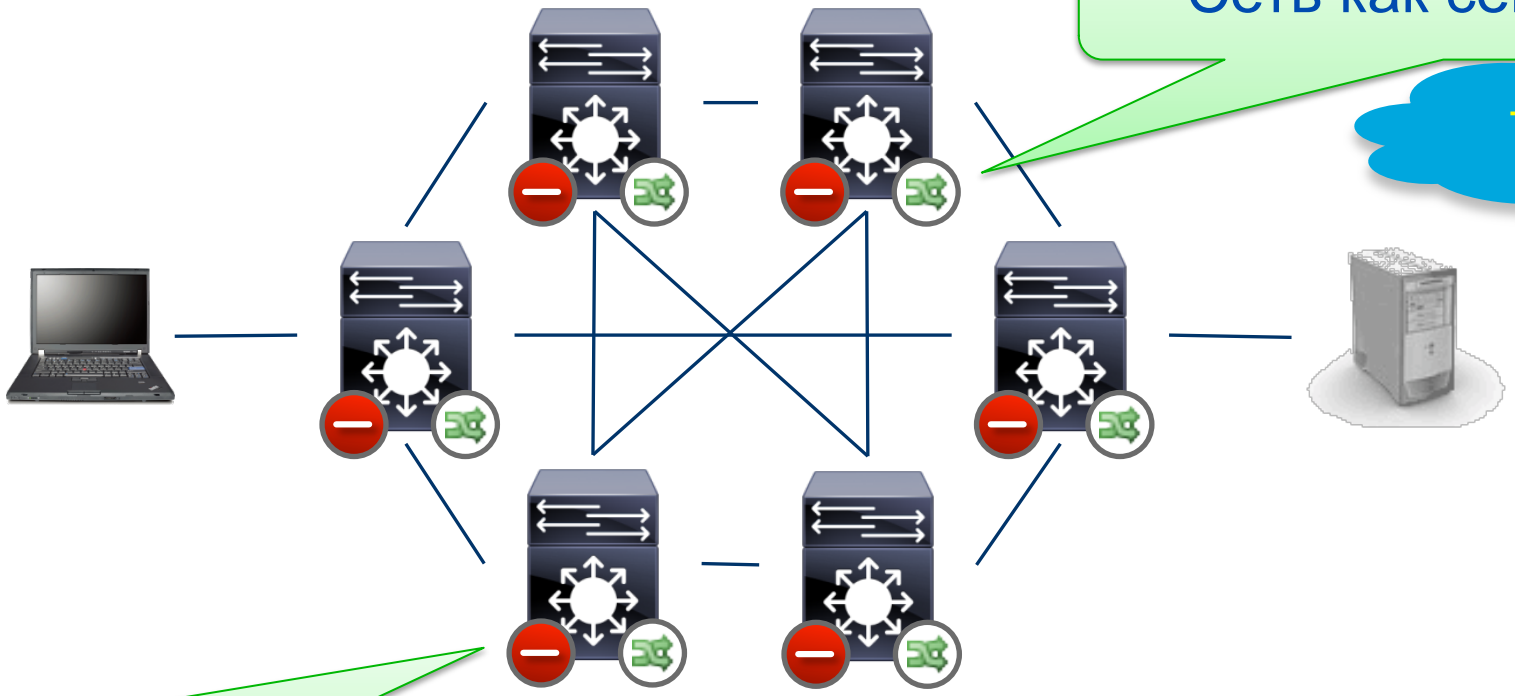
We're ready.
Are you?

Сбор телеметрии: оценка угроз



Сегментация: контроль угроз

Определение и управление политиками, поведением и контроль угроз



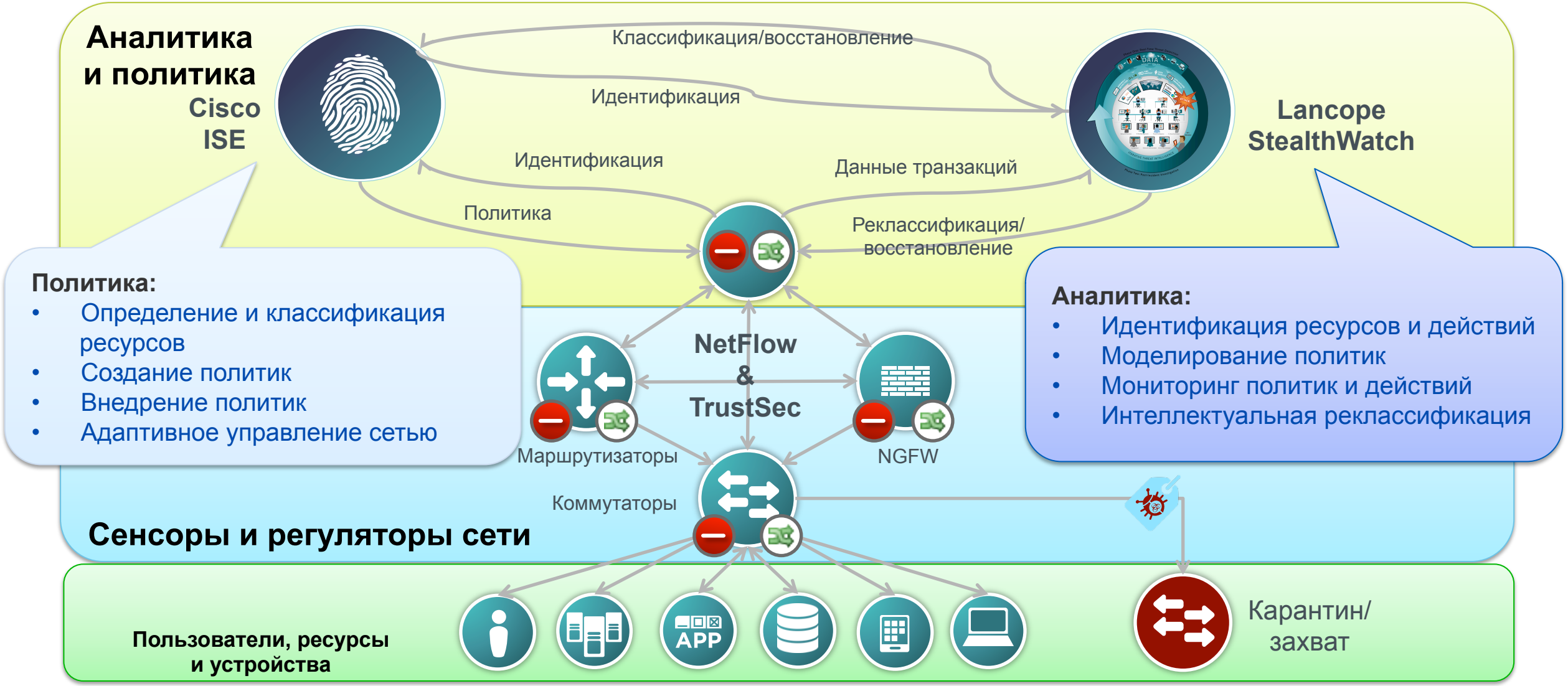
Сеть как сенсор [NaaS]

Телеметрия

Сеть как регулятор [NaaE]

Контроль благодаря телеметрии
Сегментация

Интеллектуальная сегментация



Cisco Flexible NetFlow Портолио коммутаторов

Уровень доступа

Уровень распределения

Уровень ядра

Полный Flexible NetFlow v9 и IPFIX*

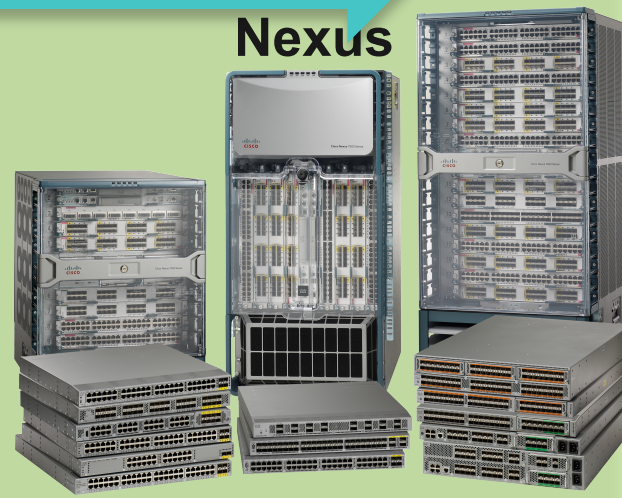
Catalyst 3850/3650

Catalyst 2960x

Catalyst 4500 Sup7E/LE/8E

Catalyst 6800/6500 Sup2T

Nexus

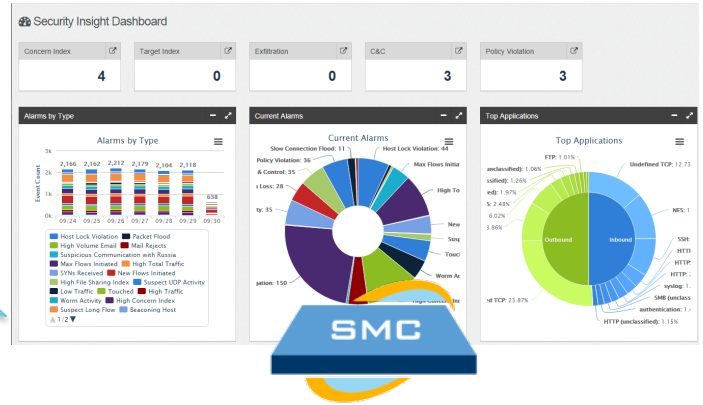


NetFlow поддерживается на 7K M картах (full / sampled), 1000V (Full Flow) и 7k (в зависимости от I/O модуля)

Обзор решения сеть как сенсор
Cisco StealthWatch + Cisco NetFlow

Корреляция в реальном времени , визуализация трафика и консолидированная отчетность

- До 25-ти сборщиков потоков



StealthWatch Management Console

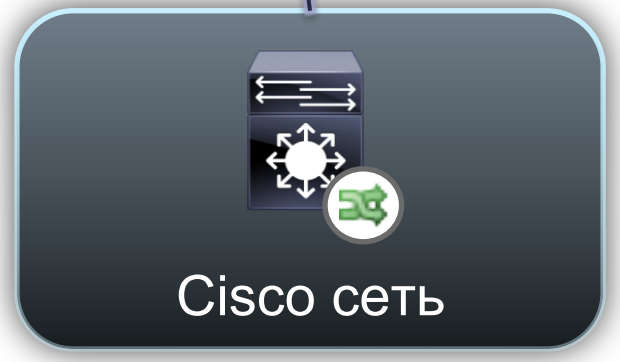
https

Сбор, хранение и анализ NetFlow записей

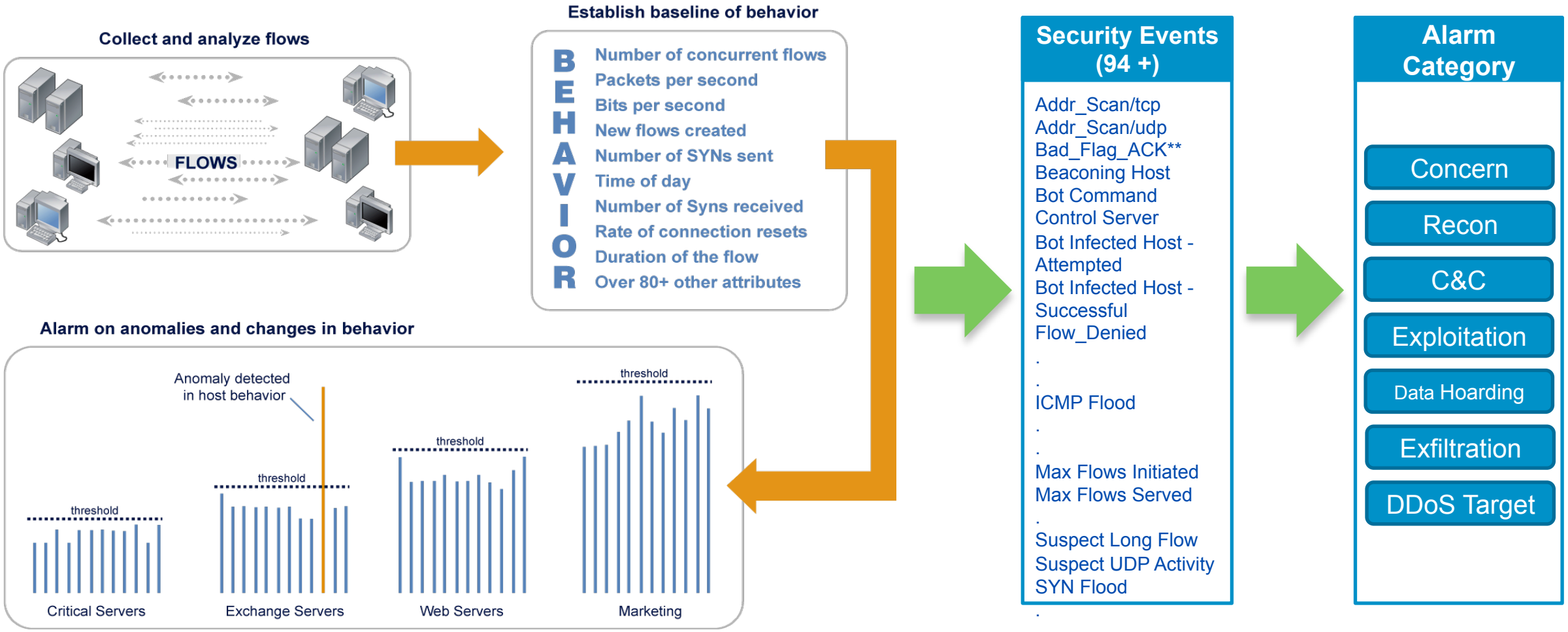
- До 2000 источников, 120K FPS

StealthWatch FlowCollector

NetFlow



Сеть как сенсор
Поведенческий анализ и обнаружение аномалий через NETFLOW



StealthWatch: Веб центр аналитики

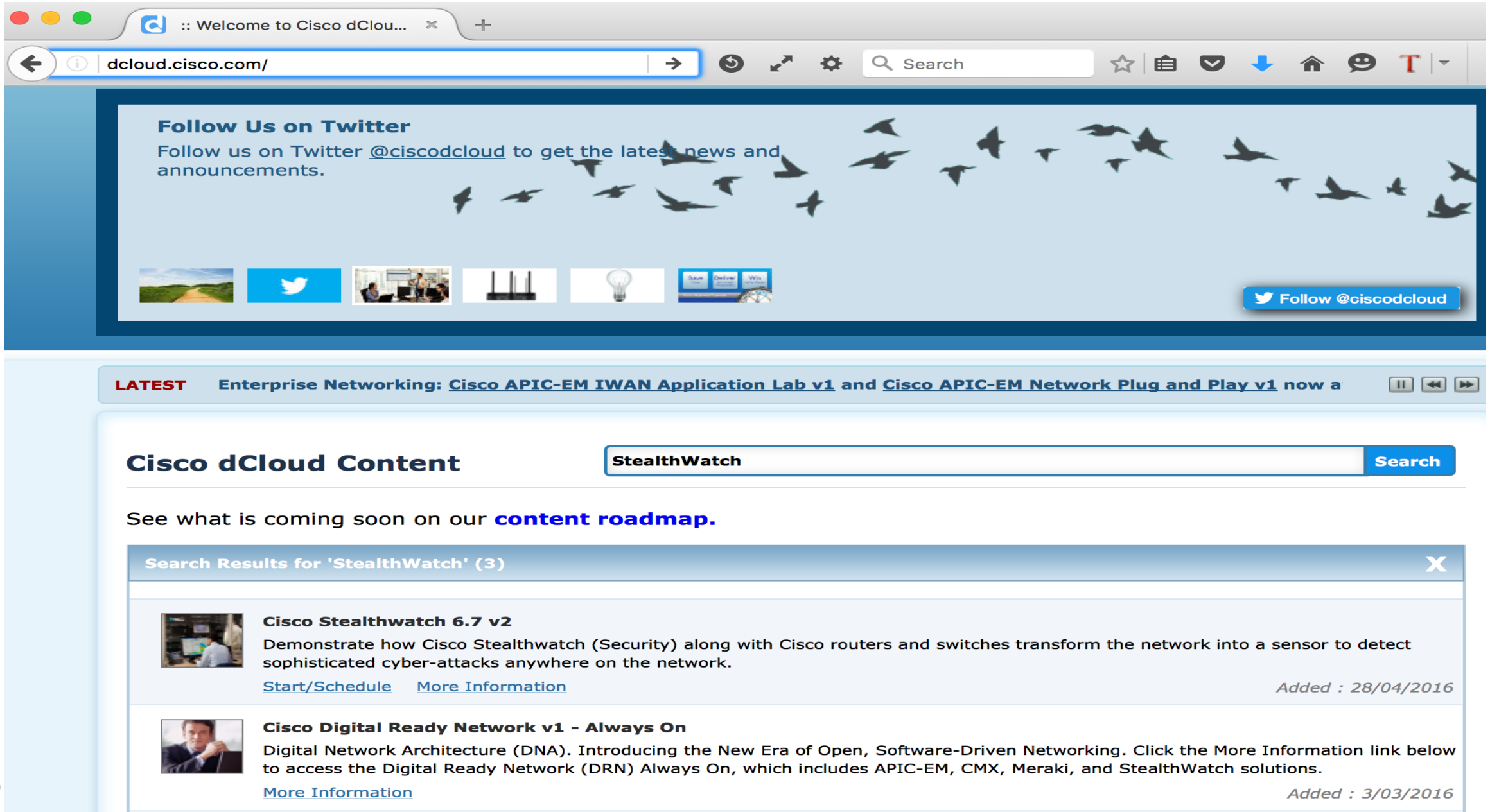
Активные Тревоги

Тревоги

Топ приложений

Тренд сбора потоков

Хочется взглянуть самому на Cisco Stealth Watch?



[Q3] Что такое Flexible NetFlow [FNF]?

Cisco Forum

Network as an Enforcer [NaaE]

[6 / 7]

We're ready.
Are you?

Как сеть может защитить?

Сеть как средство контроля

Сегментация [TrustSec]

сети для сдерживания атаки

Остановить распространение Malware, Exploitation, и свободного движения

Обмен политикой [pxGrid]

для защиты приложений и данных

Как только появился в сети, вся сеть знает куда тебе НЕЛЬЗЯ и кому к тебе НЕЛЬЗЯ

Упрощение [API]

политика безопасности в сети

Обновляйте и автоматизируйте развертывание Ваших средств контроля безболезненно

Сегментация с TrustSec

Программируемая система

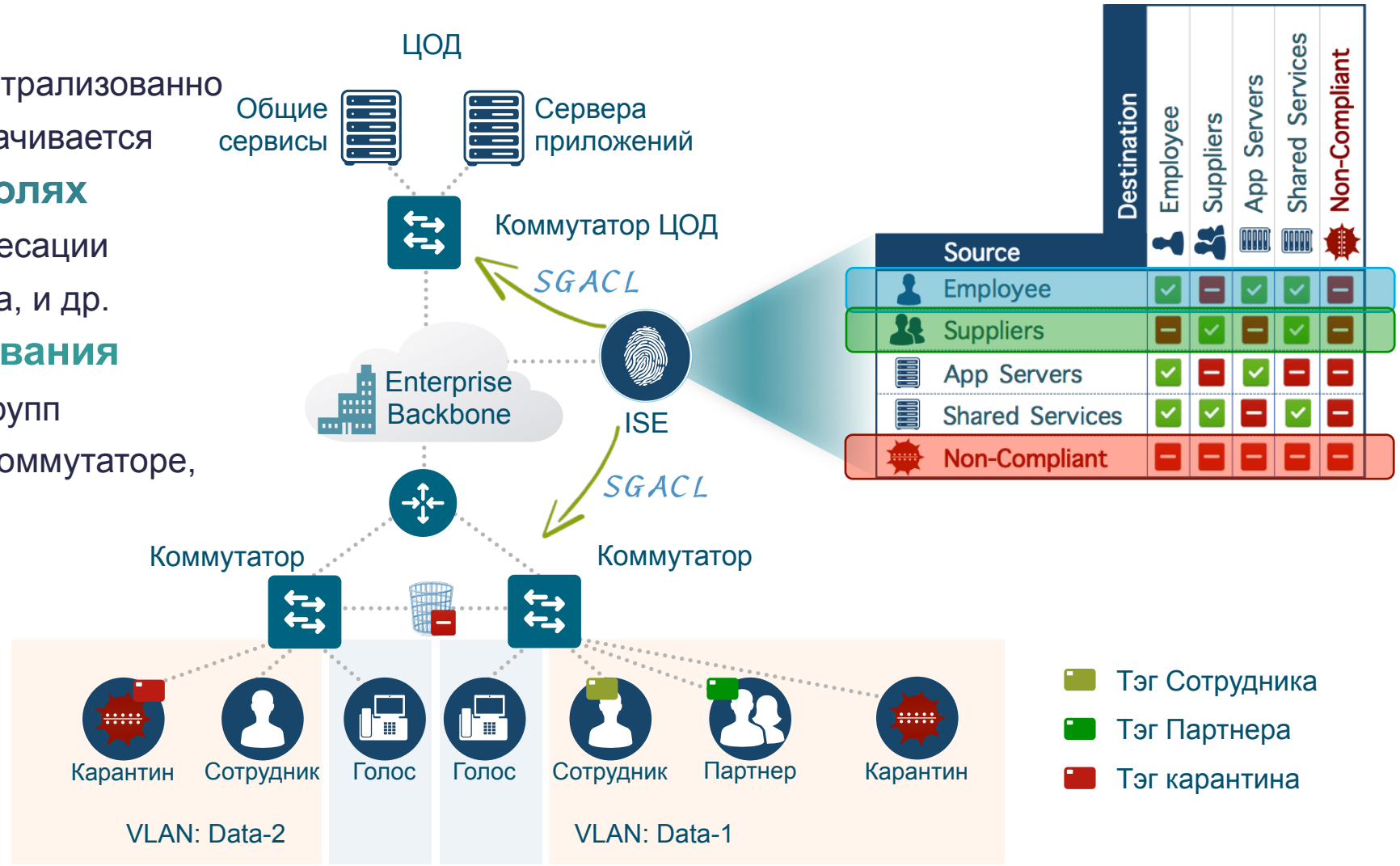
- Политика устанавливается централизованно
- Политики динамически разворачивается

Сегментация основанная на Ролях

- Независимость от сетевой адресации
- AD, LDAP атрибуты, устройства, и др.

Использование техники Тегирования

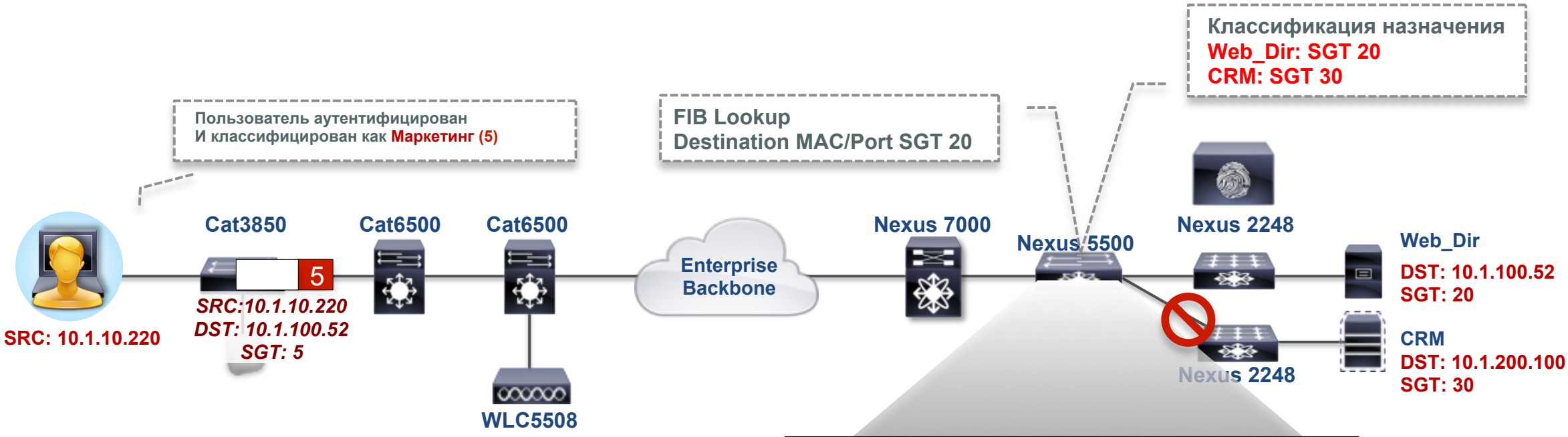
- Для обозначении логических групп
- Для применения политики на коммутаторе, роутере и фаерволе



TrustSec концепция

- Классификация систем/пользователей основанная на **контексте** (роль пользователя, устройство, расположение, метод доступа)
- **Классификация основанная на контексте** распространяется через **SGT**
- SGT используется МСЭ, роутерами и коммутаторами для интеллектуального перенаправления или блокировки

Применение политик - Security Group ACL (SGACL)

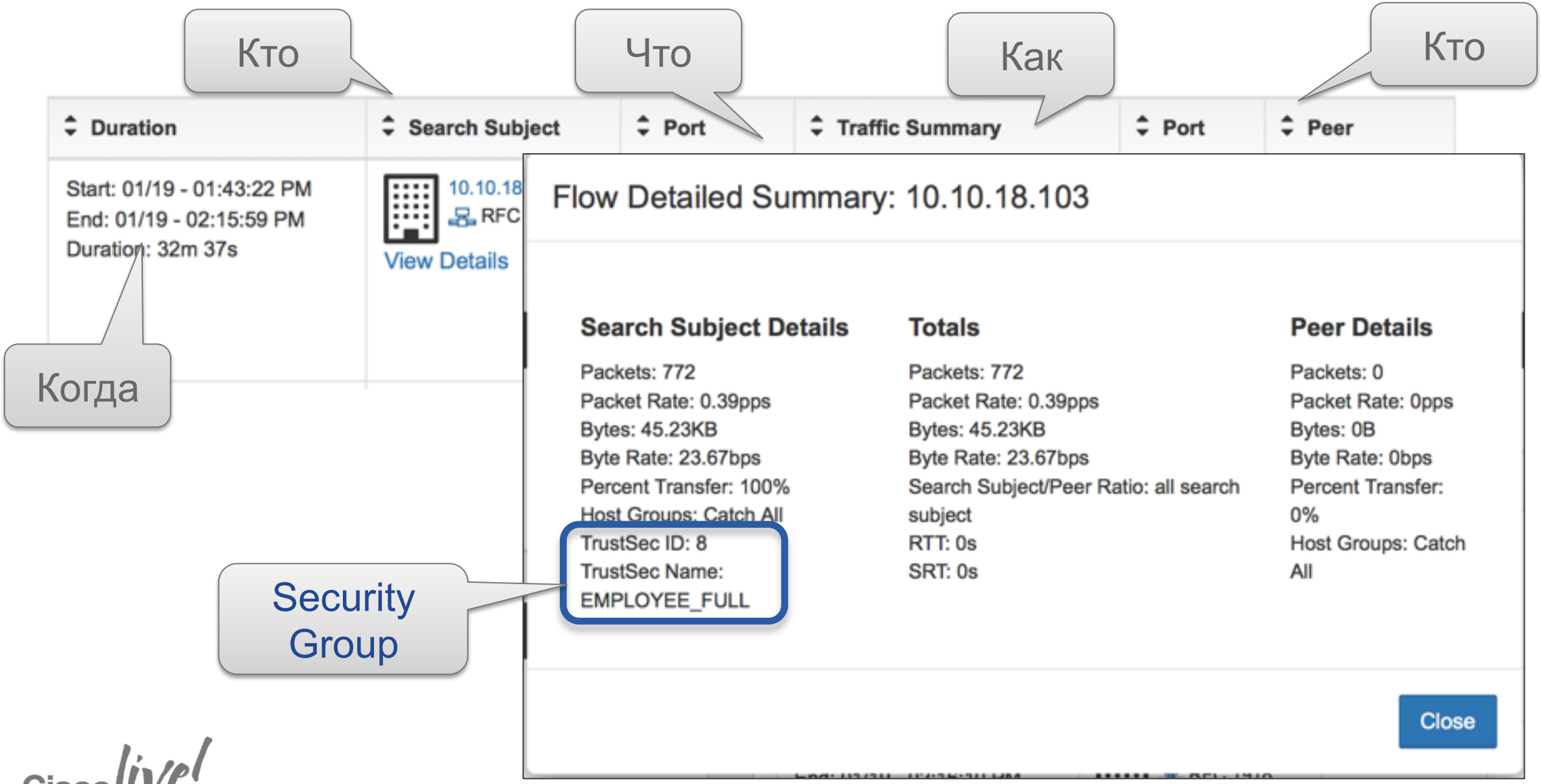


SRC\DST	Web_Dir (20)	CRM (30)
Маркетинг (5)	SGACL-A	SGACL-B
BYOD (7)	Deny	Deny

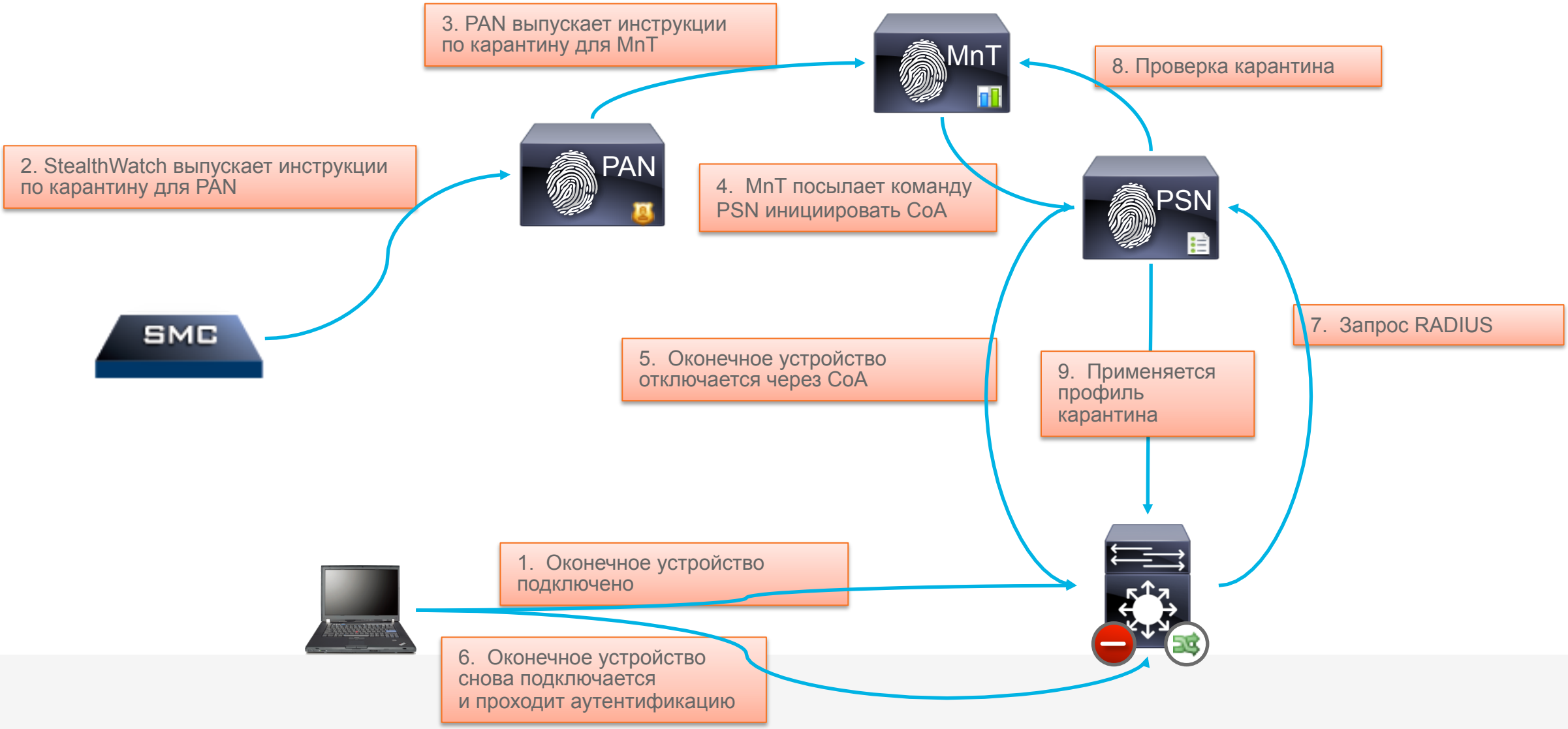
TrustSec поля внутри NetFlow

```
Router# show flow monitor CYBER-MONITOR cache
...
IPV4 SOURCE ADDRESS:            10.1.100.82
IPV4 DESTINATION ADDRESS:       8.8.8.100
TRNS SOURCE PORT:               0
TRNS DESTINATION PORT:          2048
INTERFACE INPUT:                Gi0/0/0
FLOW DIRECTION:                 Input
FLOW CTS SOURCE GROUP TAG:      1001
FLOW CTS DESTINATION GROUP TAG: 1000
IP PROTOCOL:                    1
ipv4 next hop address:          8.8.8.100
tcp flags:                      0x00
interface output:               Gi0/0/2
counter bytes:                  120
counter packets:                2
timestamp first:                05:29:17.398
timestamp last:                 05:29:18.396
ip dscp:                        0x00
ip ttl min:                     123
ip ttl max:                     123
application name:               layer7 ping
...
```

Новое в StealthWatch 6.7 – SGT Теги



Поток трафика в карантине



Cisco Forum

Собираем всё в архитектуру

[7 / 7]

We're ready.
Are you?

Сеть как сенсор и средство контроля

Масштабируемая безопасность по политикам

Упрощение политики безопасности, Автоматизация настроек и управление изменениями

Сеть как сенсор безопасности

Глубокий взгляд для мониторинга активностей,
Обнаружение угроз, Соответствие требованиям

(*Использование NetFlow*)

Сеть как средство контроля

Целостная политика доступа и сегментации во всей сети

(*Используя TrustSec*)

Сеть как сенсор и средство контроля

Улучшить видимость угроз

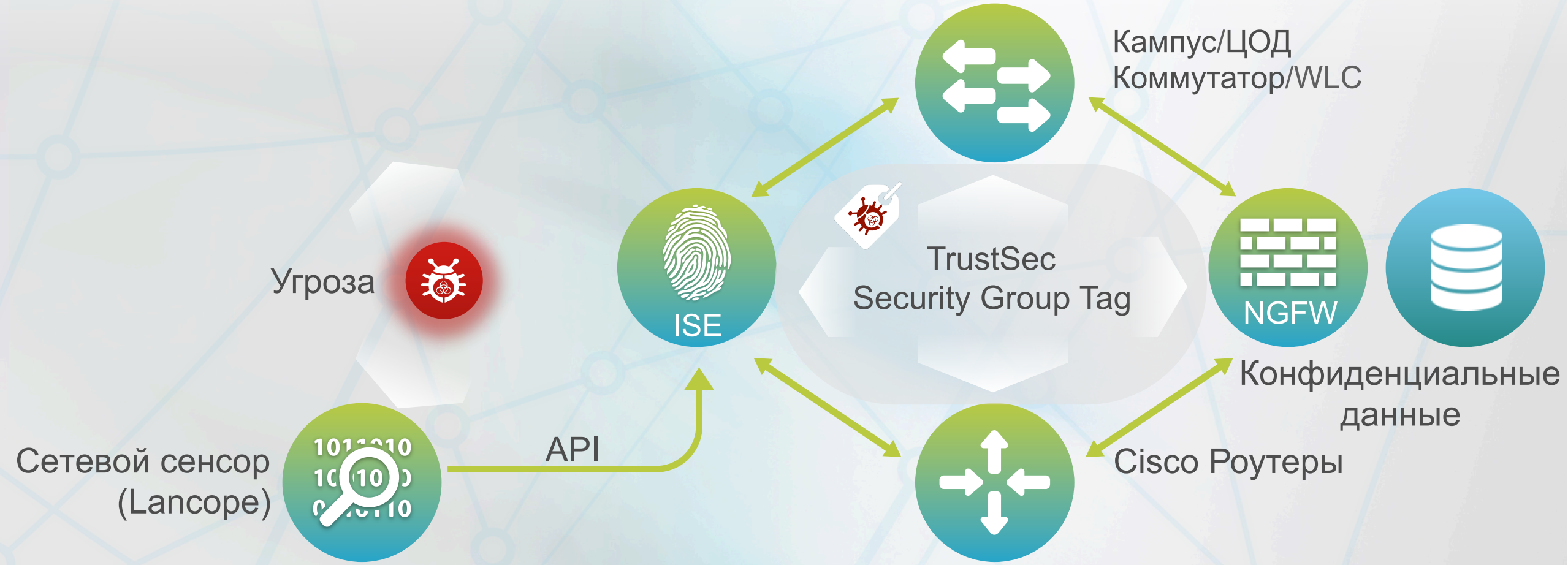
NetFlow + Lancope +
ISE для Контекста

Уменьшить площадь атаки

ISE + TrustSec

Архитектура безопасности

Объединим встроенные и распределенные инструменты борьбы с угрозами



Сетевые сенсоры

Обмен политикой и контекстом

Сетевой контроль

[Q4] OpenFlow?

Cisco Forum

SDN подход к ответвлению трафика для сетей без NetFlow и для многих других нужд ИБ

[8 / 7]

We're ready.
Are you?

Cisco Nexus Data Broker

Scalable Network Traffic Monitoring Solution

Andrii Ovrashko
Systems Engineer

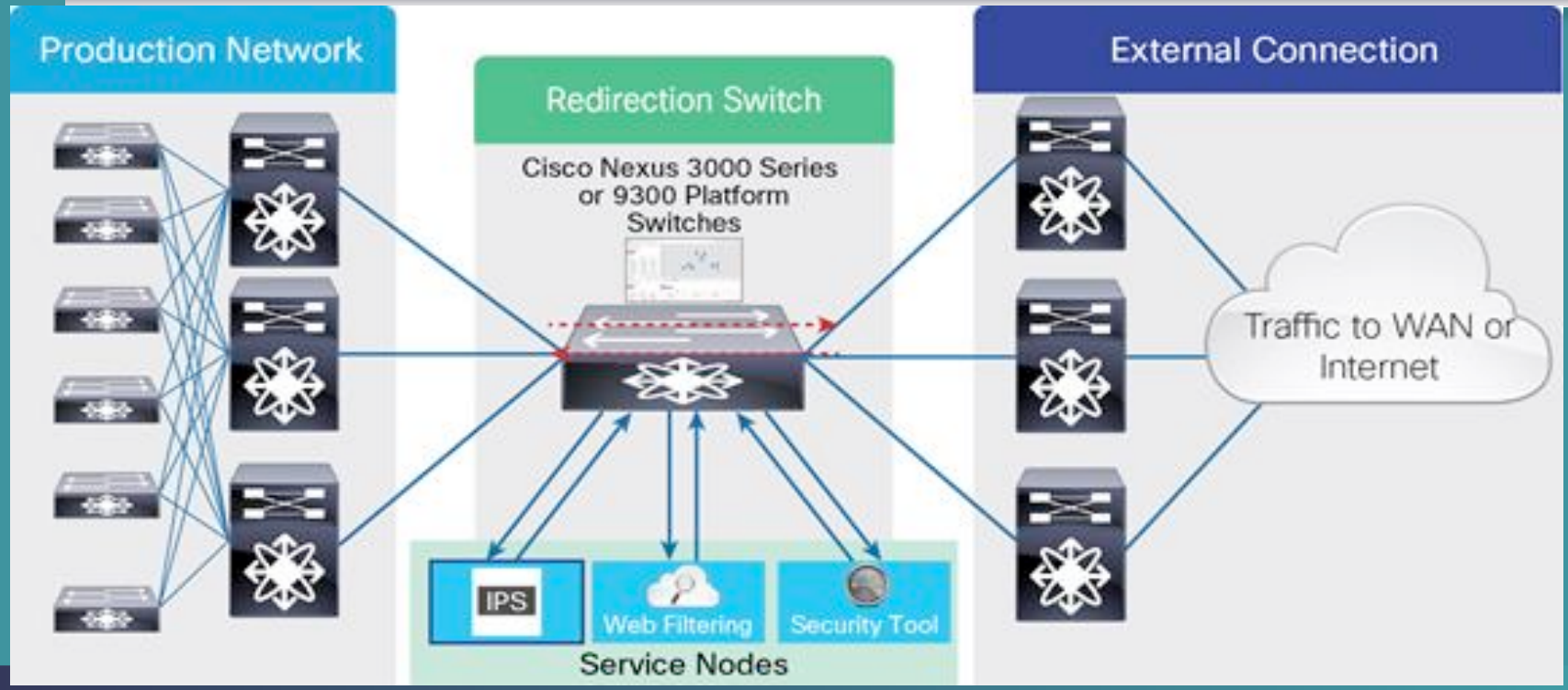
Проблематика: – *“Keeping up with the exploding network traffic”*

Потребность:

- Понимать производительность приложений
- Поддерживать соответствие требованиям внутренних и внешних регуляторов
- Отладка и изоляция доменов отказа
- Отдать средствам ИБ/ИТ копию данных

Полезность:

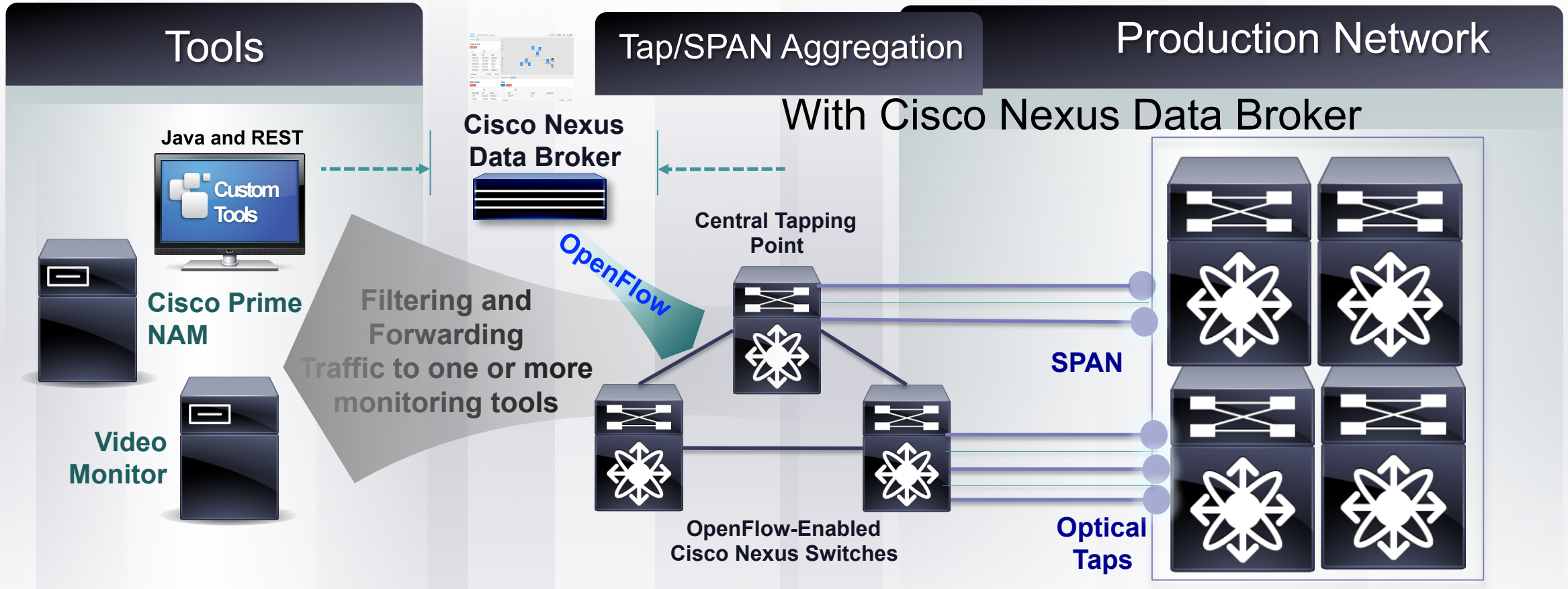
- Контроль SLA
- Проактивная идентификация потенциальных угроз и проблем.
- Минимизация рисков фин потерь.
- Предотвращение эффекта network bottlenecks
- Планирование развития емкости сети



Болевые точки

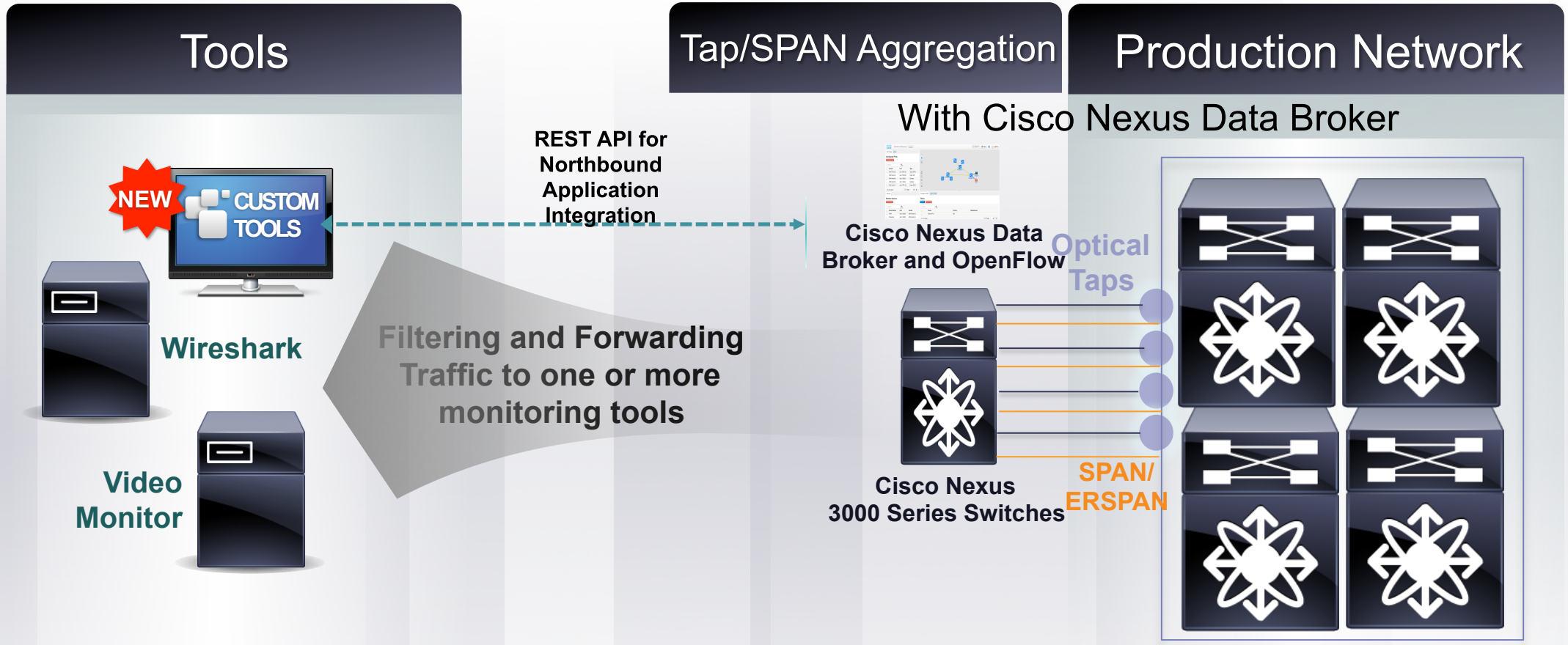
- Заоблачная стоимость проектов с матричными свичами или спец устройтвами (GigaMon, Flux, &&)
- Ограничения топологии и масштабирования матричных свичей
- Фильтрация и перенаправление статичны, а хочется по событию

Cisco Nexus Data Broker – Centralized Deployment



Cisco Nexus Data Broker replaces the Purpose-Built Matrix Switch with Cisco Nexus Switches for scalable and cost-effective Tap/SPAN Aggregation

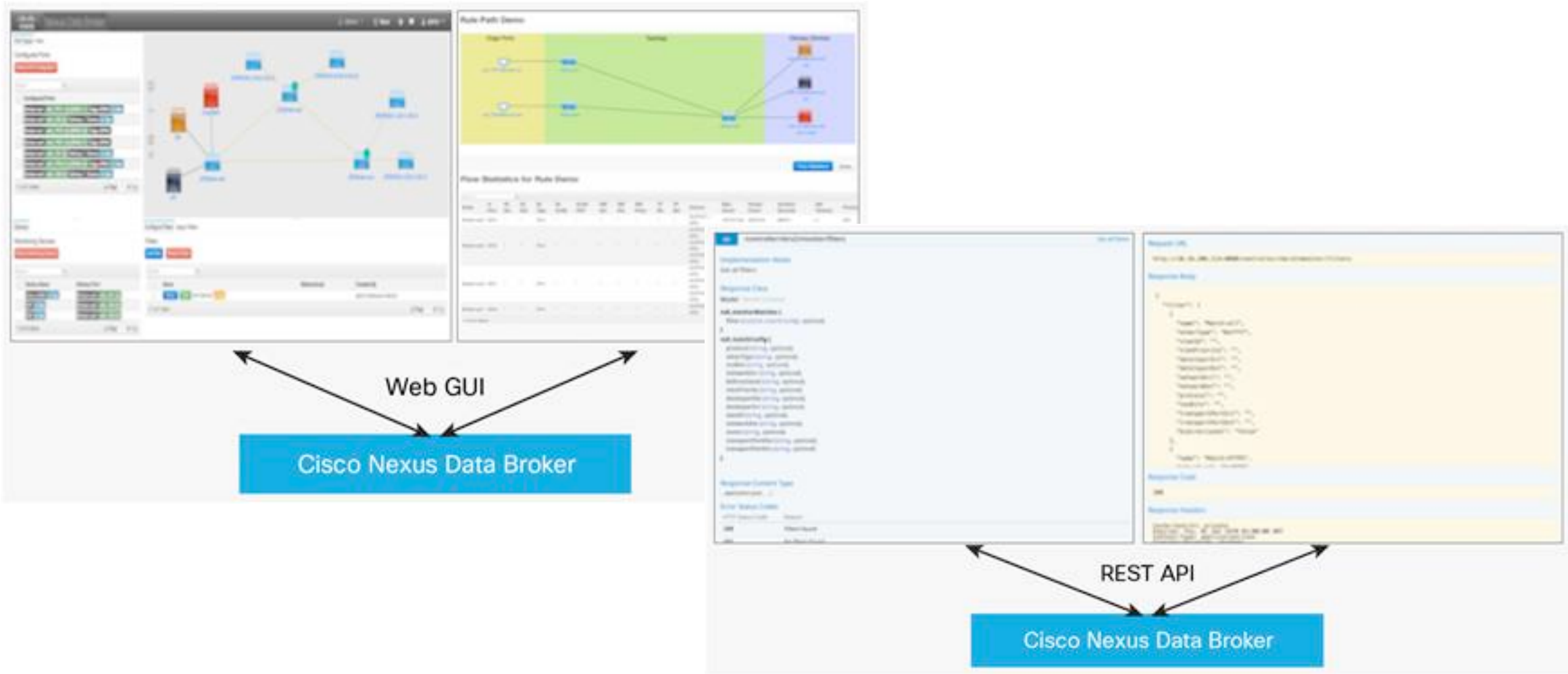
Cisco Nexus Data Broker Embedded – On Switch Deployment



Cisco Nexus Data Broker Software runs

on a OpenFlow-Enabled Cisco Nexus* series switch

Интерфейс управления: Web GUI или REST API

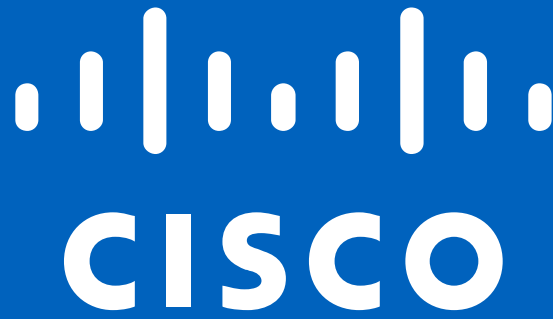


Device Model	Cisco Nexus Data Broker Software	Deployment Mode Supported	Supported Use Cases
Cisco Nexus 3100 platform	All Cisco Nexus Data Broker releases	Centralized and Embedded	TAP and SPAN aggregation and inline monitoring
Cisco Nexus 3164Q Switch	Cisco Nexus Data Broker 2.2 and later	Centralized and Embedded	TAP and SPAN aggregation only
Cisco Nexus 3500 Series	Cisco Nexus Data Broker 2.0 and later	Centralized and Embedded	TAP and SPAN aggregation only
Cisco Nexus 9300 platform	Cisco Nexus Data Broker 2.1 and later	Centralized and Embedded	TAP and SPAN aggregation and inline monitoring
Cisco Nexus 9500 platform	Cisco Nexus Data Broker 2.1 and later	Centralized only	TAP and SPAN aggregation only
Cisco Nexus 3200 platform	Cisco Nexus Data Broker 3.0	Centralized and Embedded	TAP and SPAN aggregation only

Благодарю за внимание!!

Вопросы – ответы

Thank you.



Облачные демо сценарии (лабы)

- **dcloud.**cisco.com

Сайт для разрабочиков (API и прочее)

- **devnet.**cisco.com