Защита от современных угроз с помощью SourceFire FirePOWER и Cisco CTD

Андрей Москвитин
Специалист по решениям ИБ, Cisco
amoskvit@cisco.com

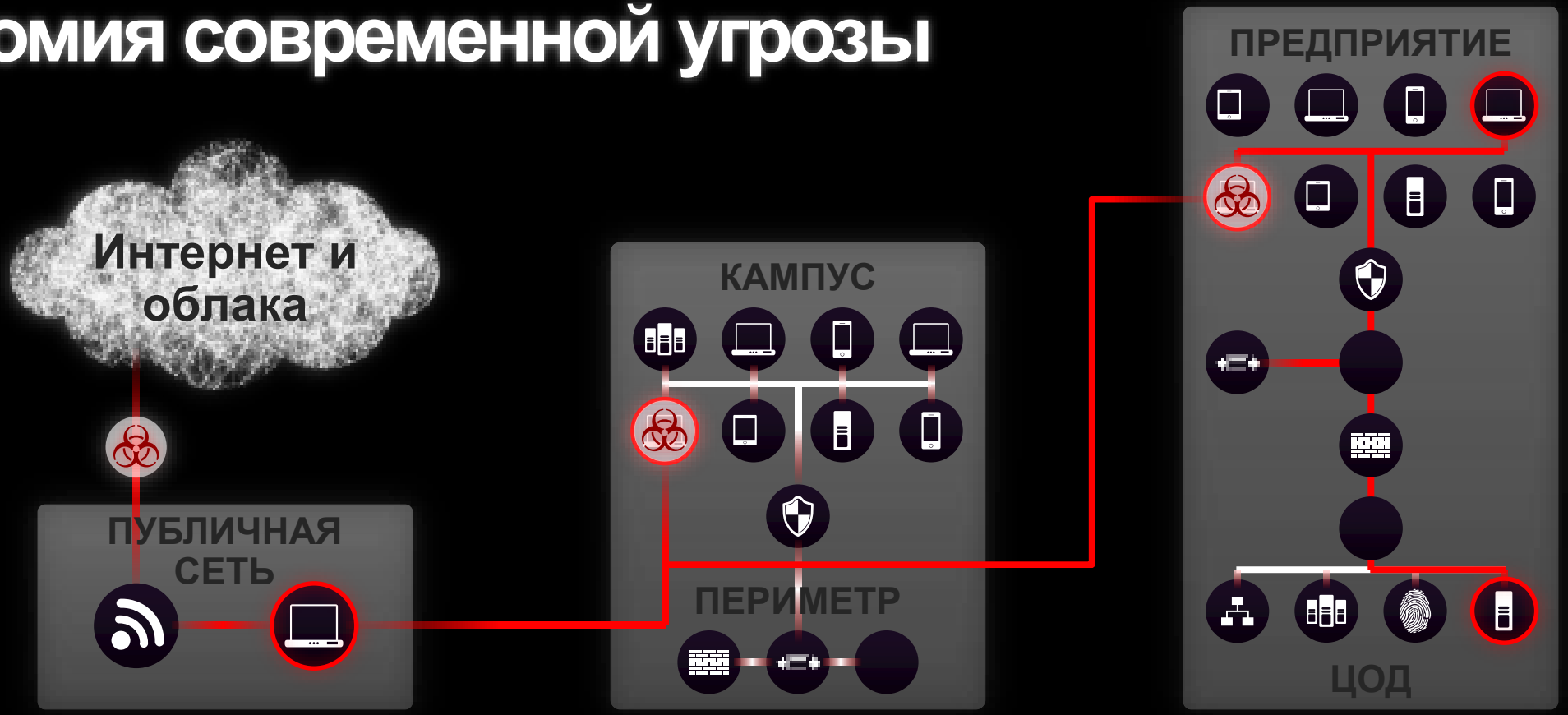
Текущие проблемы безопасности

Изменение бизнес-моделей

Динамический ландшафт угроз

Сложность и фрагментация

Анатомия современной угрозы



Заражение точки входа происходит за пределами предприятия

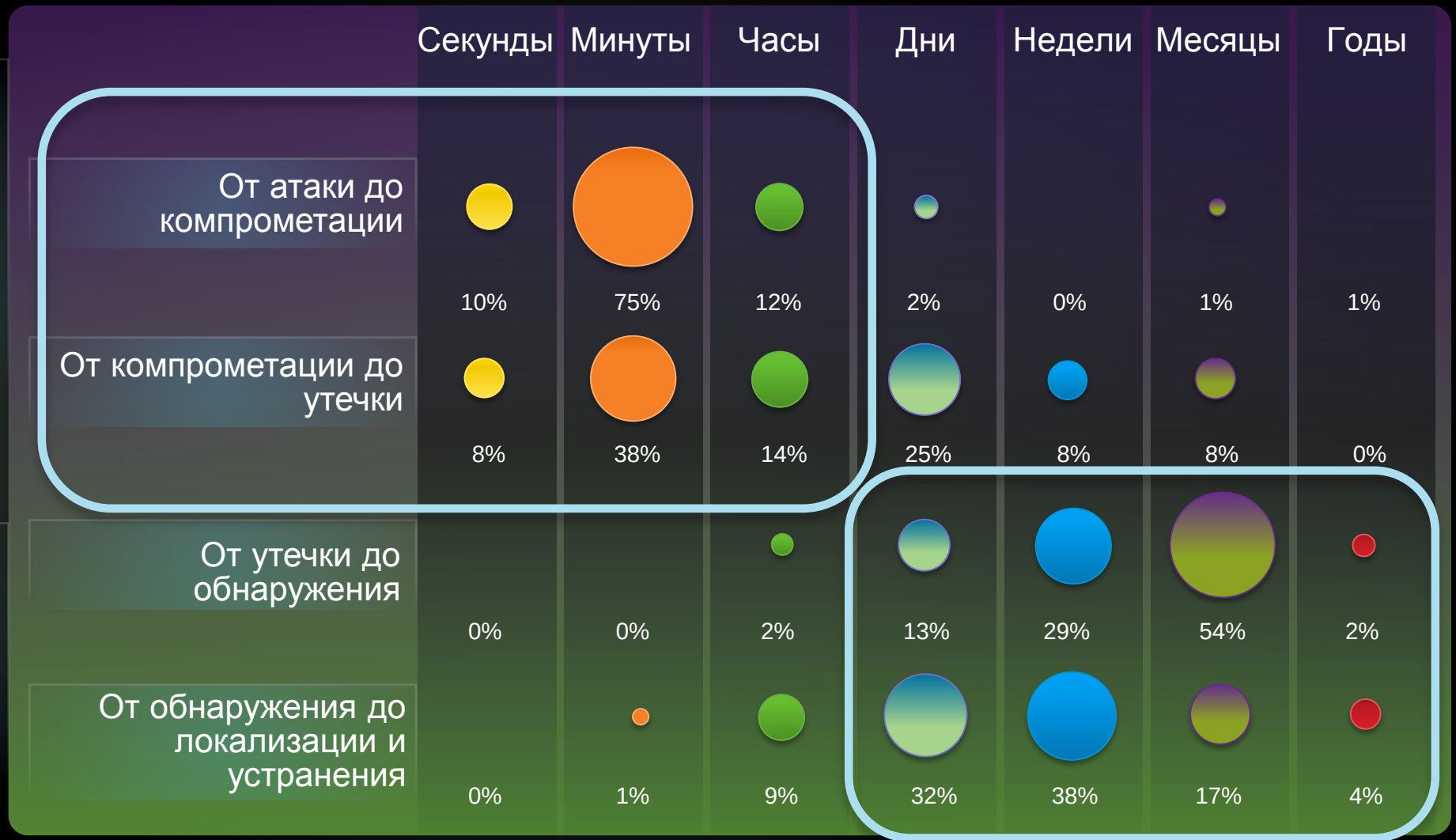
Продвинутые угрозы обходят средства защиты периметра

Угроза распространяется по сети и захватывает как можно больше данных

Время не на нашей стороне

Взломы осуществляются за минуты

Обнаружение и устранение занимает недели и месяцы



Временная шкала событий в % от общего числа взломов

Источник: 2012 Verizon Data Breach Investigations Report

Если бы Вы знали что будете взломаны действовали ли бы Вы иначе?

Новая модель безопасности

Всеобъемлющий портфель решений в области ИБ

МСЭ и NGFW

- Cisco ASA / ASA-SM
- Cisco ISR / ASR Sec
- FirePOWER NGFW
- Meraki MX

IPS и NGIPS

- Cisco IPS
- Cisco wIPS
- Cisco ASA Module
- FirePOWER NGIPS

Advanced Malware Protection

- FireAMP
- FireAMP Mobile
- FireAMP Virtual
- AMP для FirePOWER

Интернет-безопасность

- Cisco WSA / vWSA
- Cisco Cloud Web Security

Безопасность электронной почты

- Cisco ESA / vESA
- Cisco Cloud Email Security

NAC + Identity Services

- Cisco ISE / vISE
- Cisco ACS

VPN

- Cisco AnyConnect
- Cisco ASA
- Cisco ISR / RVPN

UTM

- Meraki MX

Мониторинг инфраструктуры

- Cisco Cyber Threat Defense

Policy-based сеть

- Cisco TrustSec
- Cisco ISE
- Cisco ONE

Secure DC

- Cisco ASA / 1000v / ASAv / VSG
- Cisco TrustSec

Контроль приложений

- Cisco ASA NGFW / AVC
- Cisco IOS AVC / NBAR
- Cisco SCE / vSCE
- FirePOWER NGFW

#1 на рынке ИБ ЦОДов
(Источник: Infonetics)

Лидер Gartner Magic Quadrant
(Email Security, Web Security, Network Access, SSL, IPS)

Безопасность стала одним из 5-ти основных приоритетов компании

#1 на рынке сетевой безопасности
(Источник: Infonetics)

Cisco Security Momentum

Существенные инвестиции в R&D, M&A & людей

Решения Sourcefire

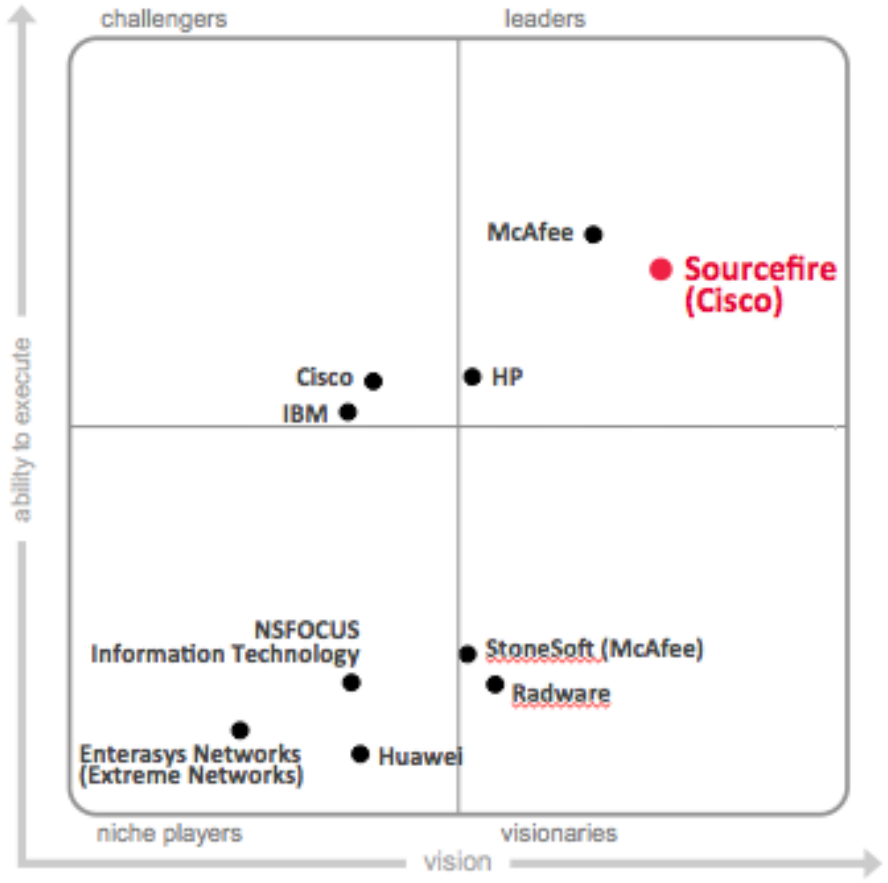
Sourcefire – эксперты в области ИБ

- Гениальная команда
- Больше 10 лет на рынке
- 6 лет подряд лидирует в квадратах Gartner
- Защищает компании в более чем 180 странах
- Инновации: 41+ патент получен или в разработке
- Open source проекты - Snort, ClamAV, Razorback, OpenAppID

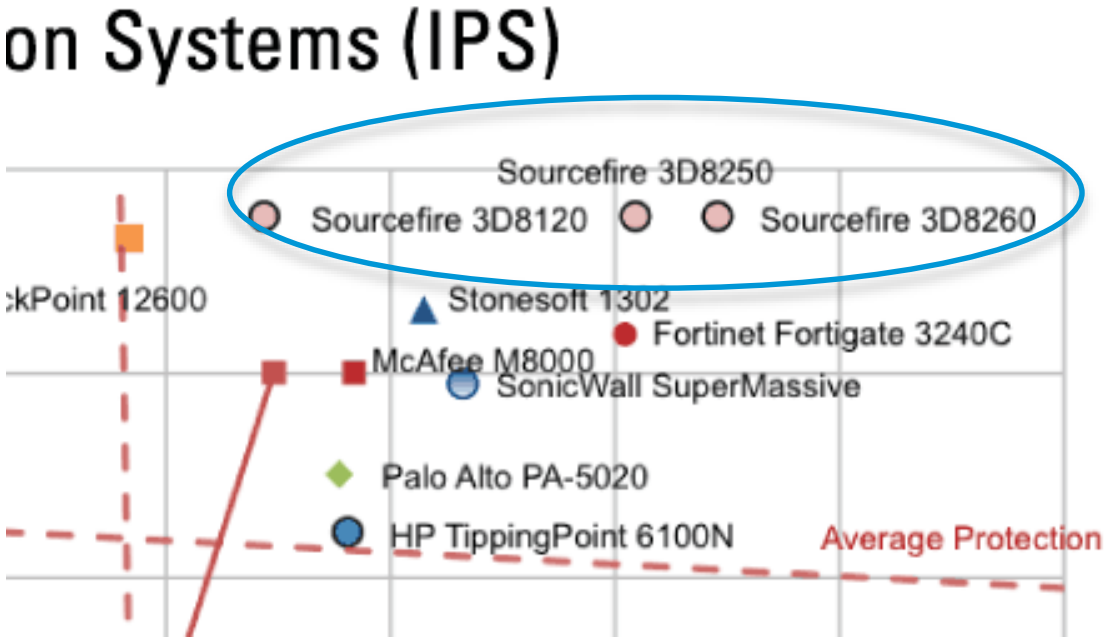
Gartner
IPS MQ Leader

Forbes
America's Fastest-Growing Tech Companies 2011

Почему лучшие?

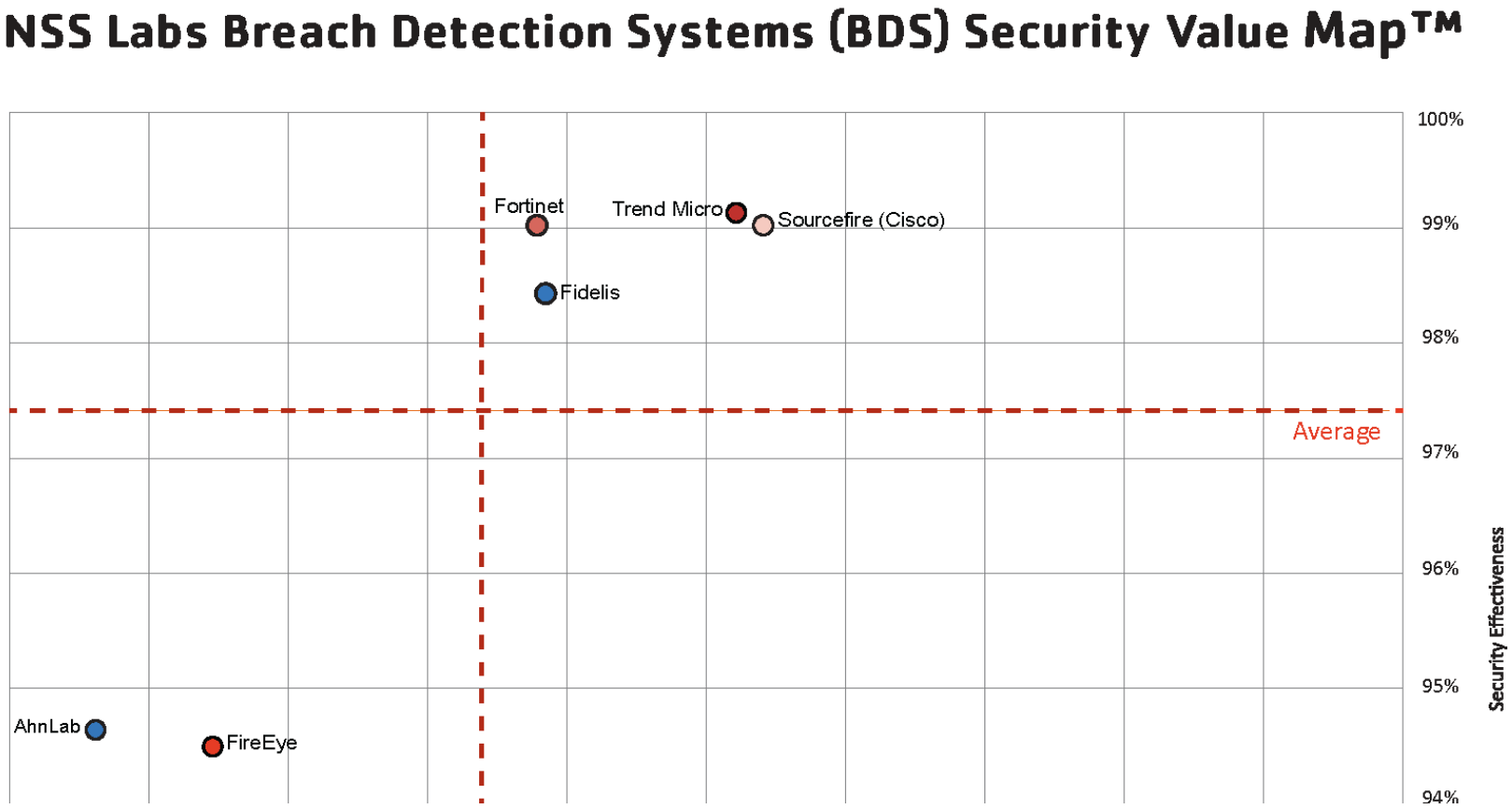


Лидер Gartner Magic Quadrant for IPS с 2006



Самый низкий TCO за защищаемый Мбит/с

Почему лучшие? (продолж.)

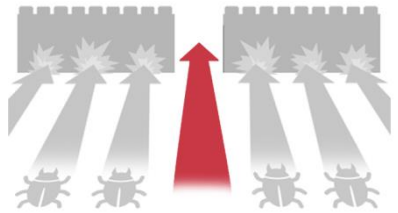
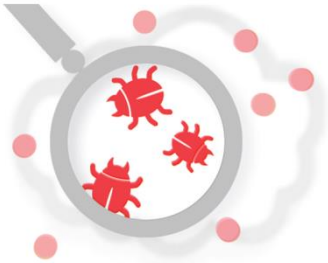


99% защита от угроз, обнаружение
100% эксплоитов, самый низкий TCO
за Мбит/с

Sourcefire – решения по обеспечению безопасности

fireSIGHT™

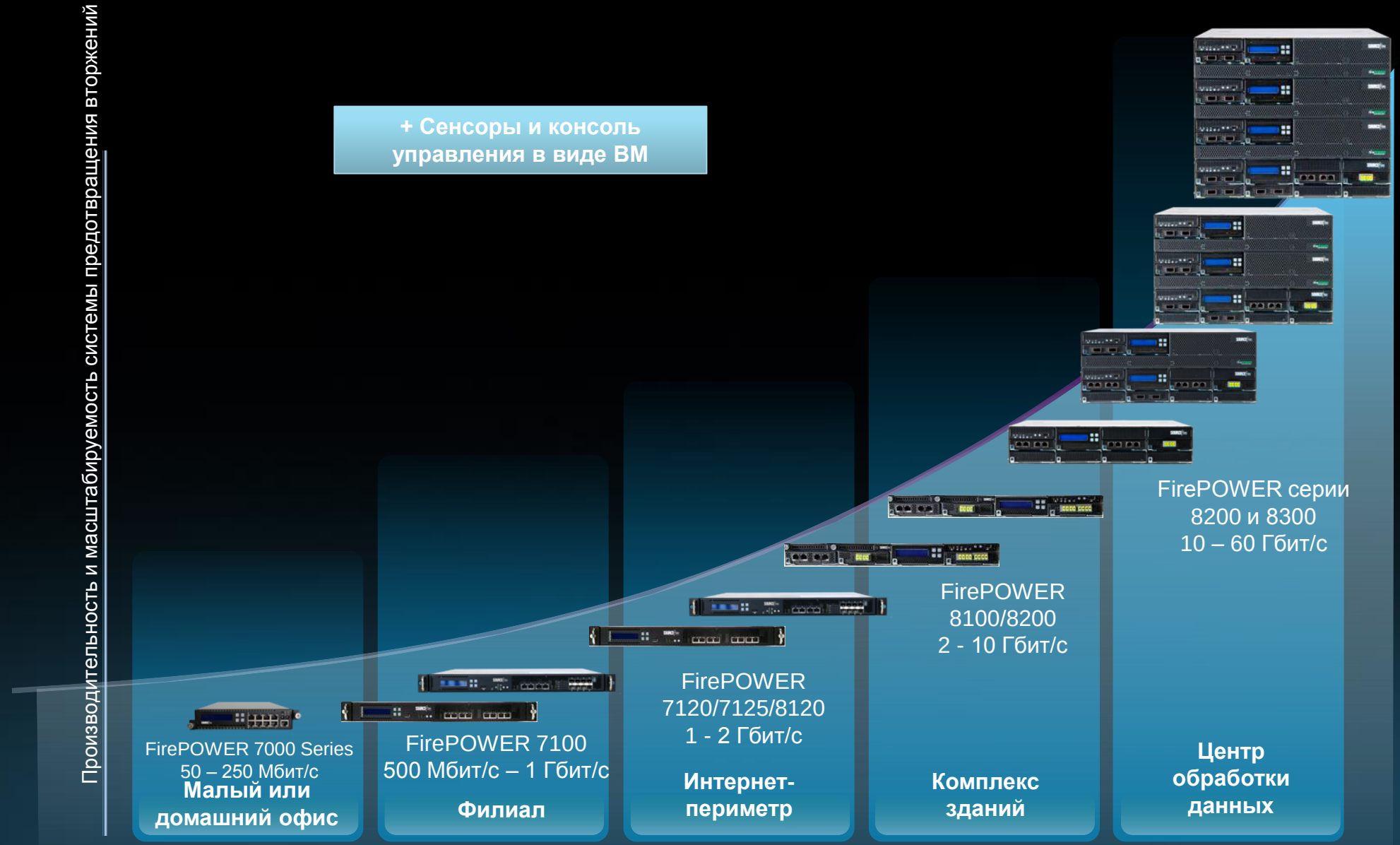
ЦЕНТР УПРАВЛЕНИЯ

ДО	ВО ВРЕМЯ	ПОСЛЕ
Вы видите, вы контролируете	Интеллектуальное противодействие и с учетом контекста	Ретроспективные средства безопасности
		
NGFW	NGIPS	AMP

firePOWER™

УСТРОЙСТВА | ВМ

Платформы и размещение в сети



Подход Sourcefire:

… непрерывный процесс до, во время и после атаки

Вы не можете защитить то, что не видите

Автоматическая настройка системы безопасности

Преобразование данных в информацию

…в режиме реального времени, в любой момент времени

В первую очередь необходимо знать, что у вас есть

Невозможно обеспечить защиту того, о чем вы не знаете

Понимание контекста

Внутри **ВАШЕЙ сети**

ЛОКАЛЬНО

Бизнес **Контекст**

- Кто
- Что
- Как
- Откуда
- Когда

Снаружи **ВАШЕЙ** сети

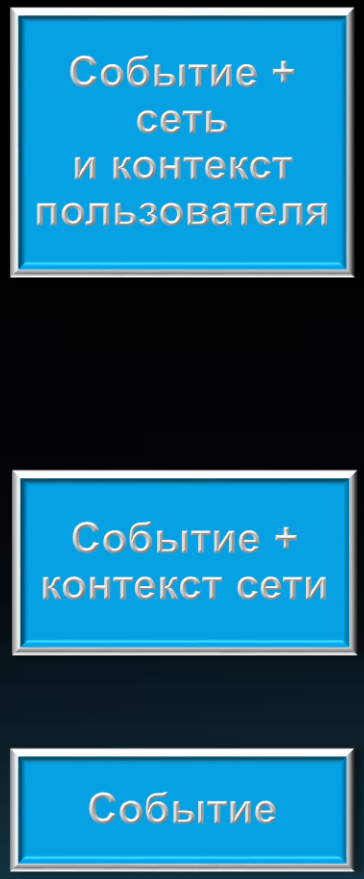
ГЛОБАЛЬНО

Ситуационный **анализ угроз**

- Репутация
- Взаимо-действие
- Приложения
- Сайты

Реализация безопасности с **локальным** и **глобальным** контекстом

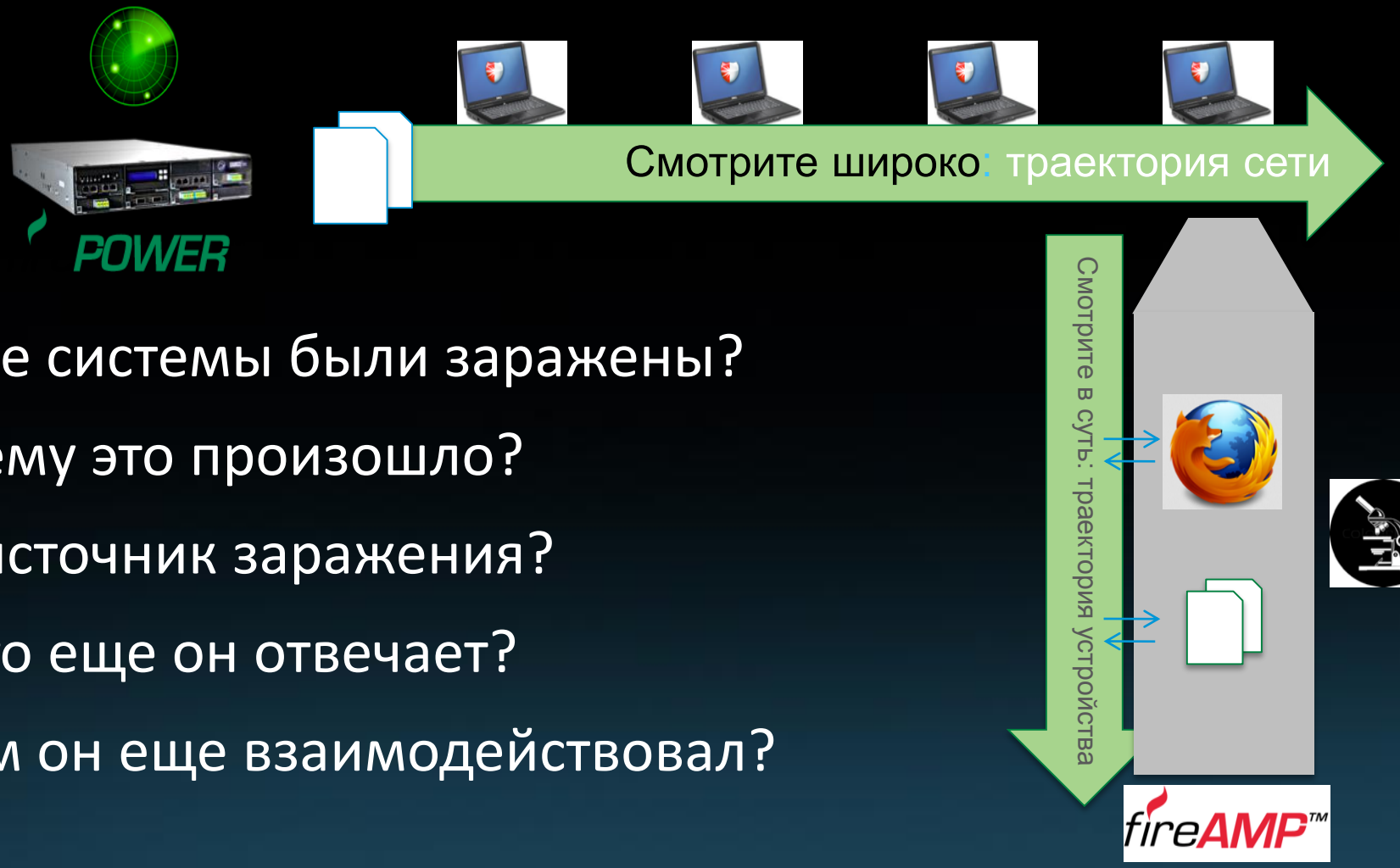
Понимание контекста (продолж.)



Событие:	**Попытка получения доступа**
Цель:	**96.16.242.135 (уязвимо)**
ОС хоста:	**Blackberry**
Приложения:	**электронная почта, браузер, Twitter**
Местоположение	**Белый дом, США**
Идентификатор пользователя:	**bobama**
Ф. И. О.	**Барак Обама**
Департамент:	**административный**
ОС хоста:	**Blackberry**
Приложения:	**электронная почта, браузер, Twitter**
Местоположение	**Белый дом, США**
	доступа
Цель:	**96.16.242.135**

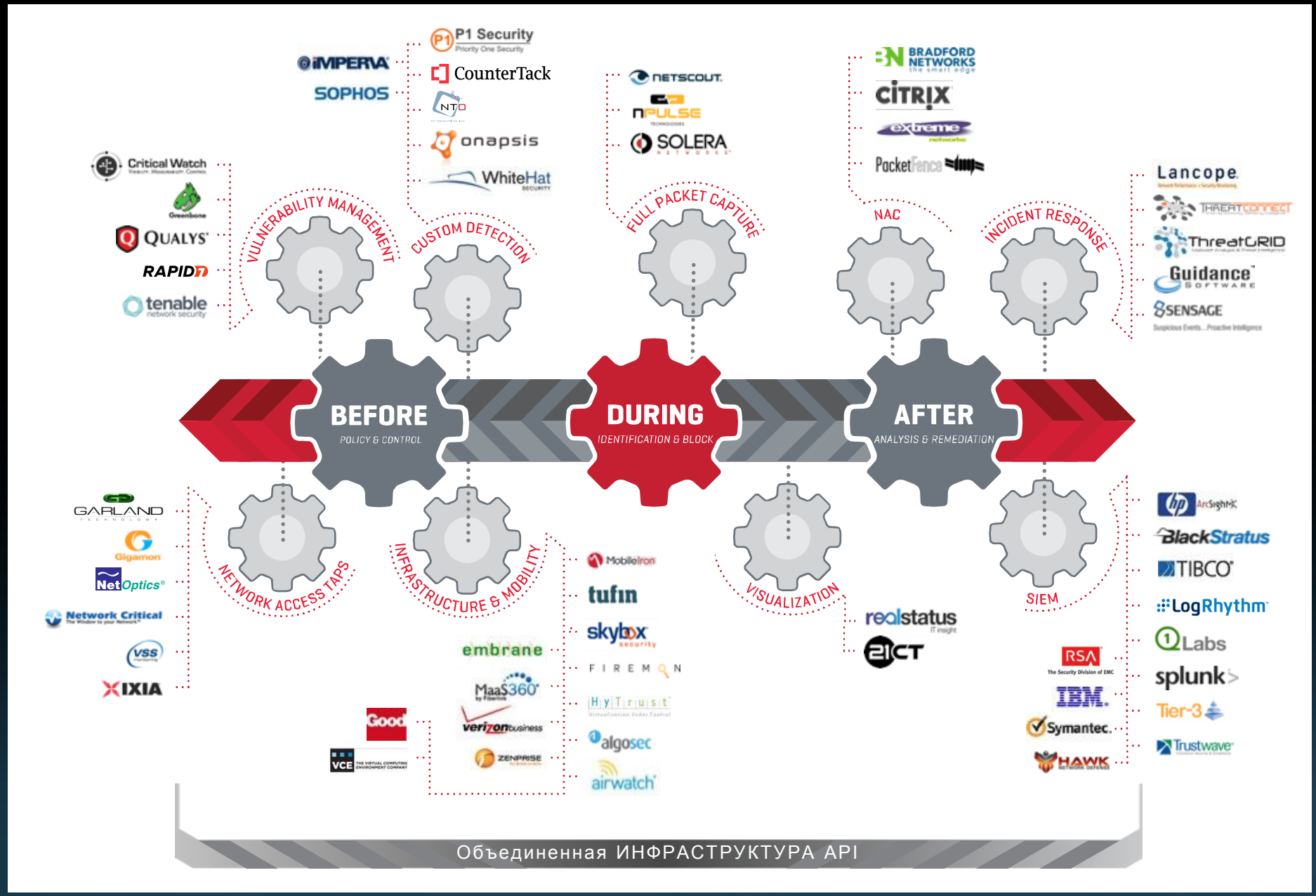
Контекст способен *фундаментально изменить* интерпретацию данных события

Анализ траектории файла и устройства – поиск источника заражения



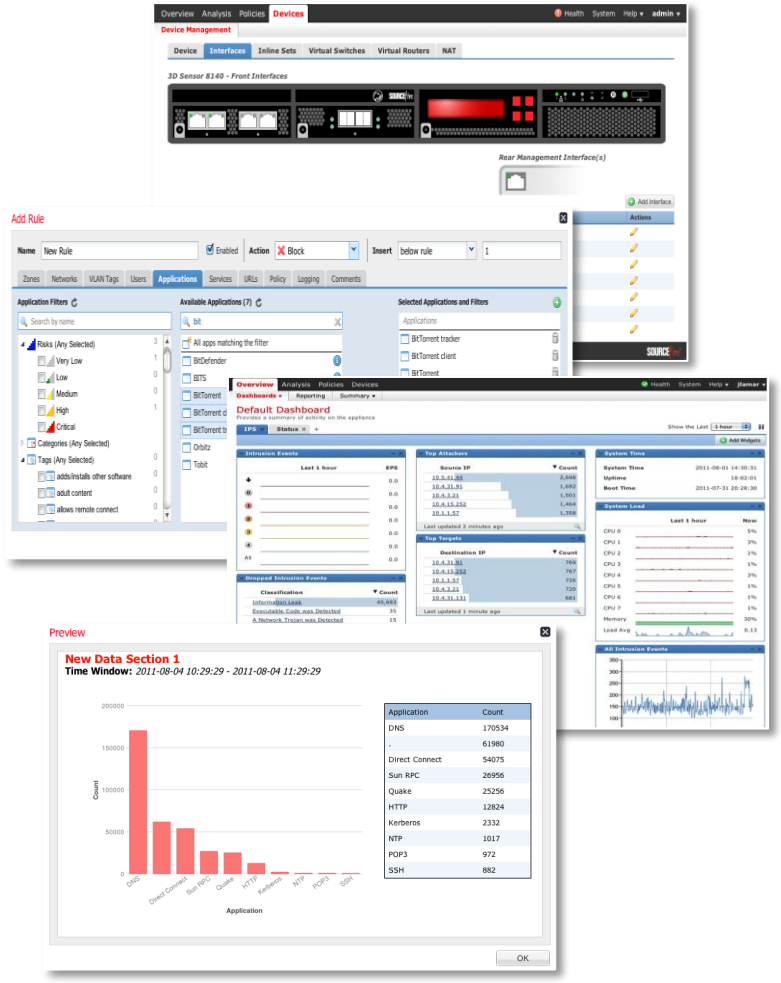
- Какие системы были заражены?
- Почему это произошло?
- Где источник заражения?
- За что еще он отвечает?
- С кем он еще взаимодействовал?

Объединенная партнерская программа Sourcefire и Cisco



Sourcefire Defense Center®

- Настраиваемая инструментальная панель
- Комплексные отчеты и оповещения
- Централизованное управление политиками
- Иерархическое управление
- Обеспечение высокой доступности
- Интеграция с существующими системами безопасности



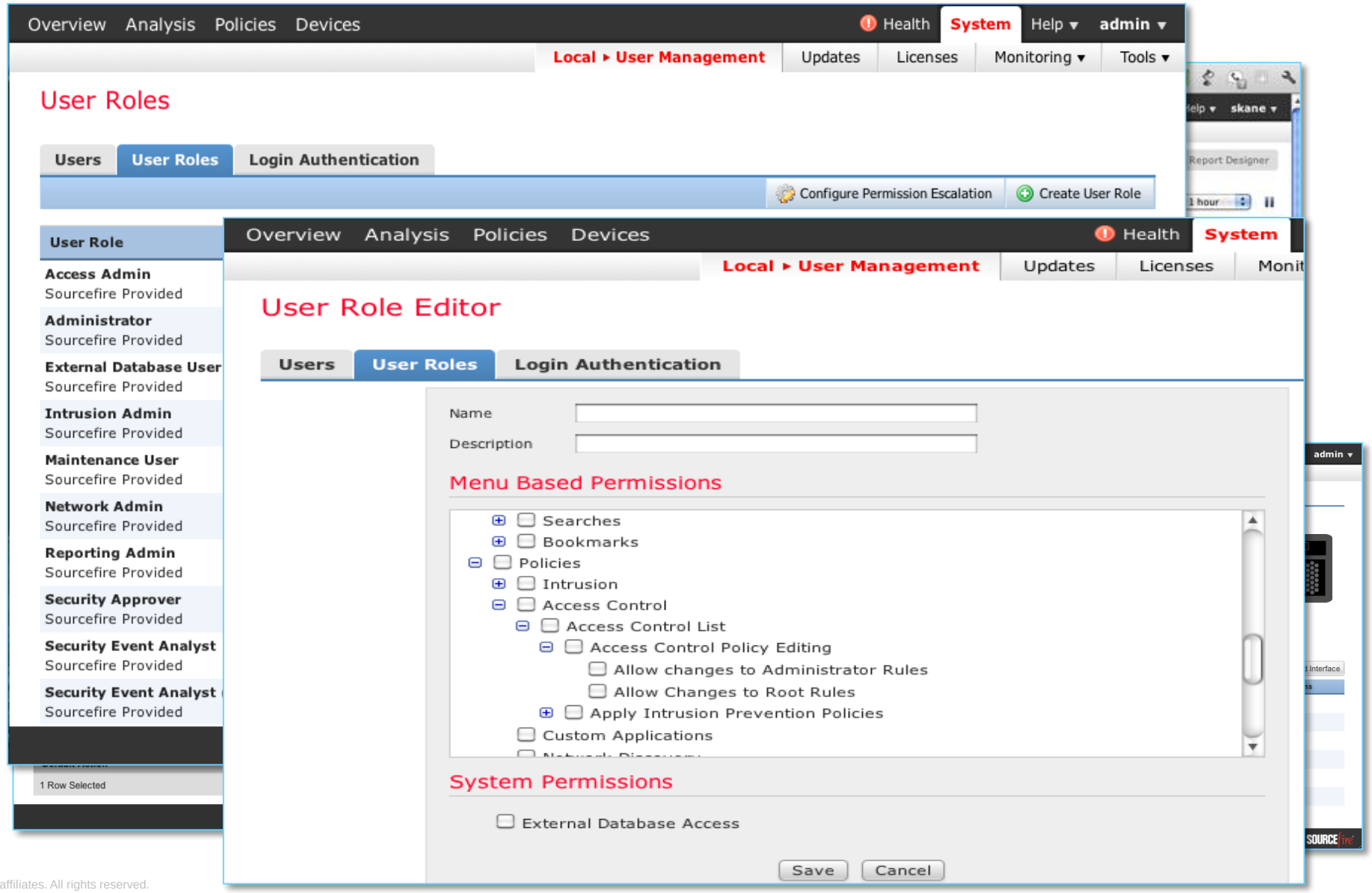
Устройства центра обеспечения защиты

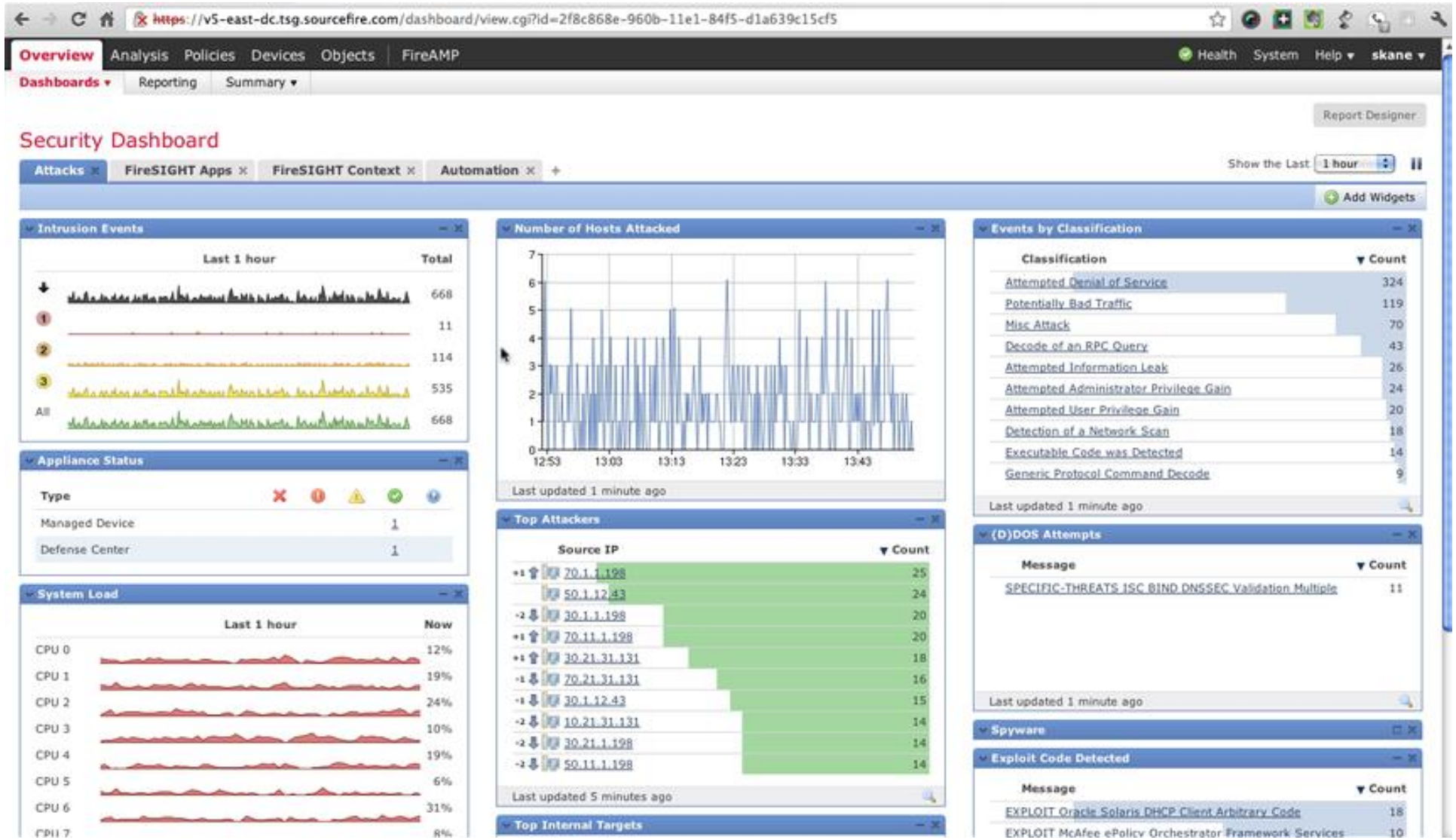
	DC750	DC1500	DC3500
Макс. число управляемых устройств*	10	35	150
Макс. число событий системы предотвращения вторжений	20 млн.	30 млн.	150 млн.
Система хранения событий	100 Гб	125 Гб	400 Гб
Макс. сетевая карта (хосты | пользователи)	2 тыс. | 2 тыс.	50 тыс. | 50 тыс.	300 тыс. | 300 тыс.
Макс. кол-во Netflow (потоков/с)	2000 потоков/с	6000 потоков/с	10000 потоков/с
Возможности высокой доступности	Дистанционное управление (LOM)	RAID 1, LOM, High Availability pairing (HA)	RAID 5, LOM, HA, резервный источник питания пер. тока

* Макс. число устройств зависит от типа сенсора и частоты событий

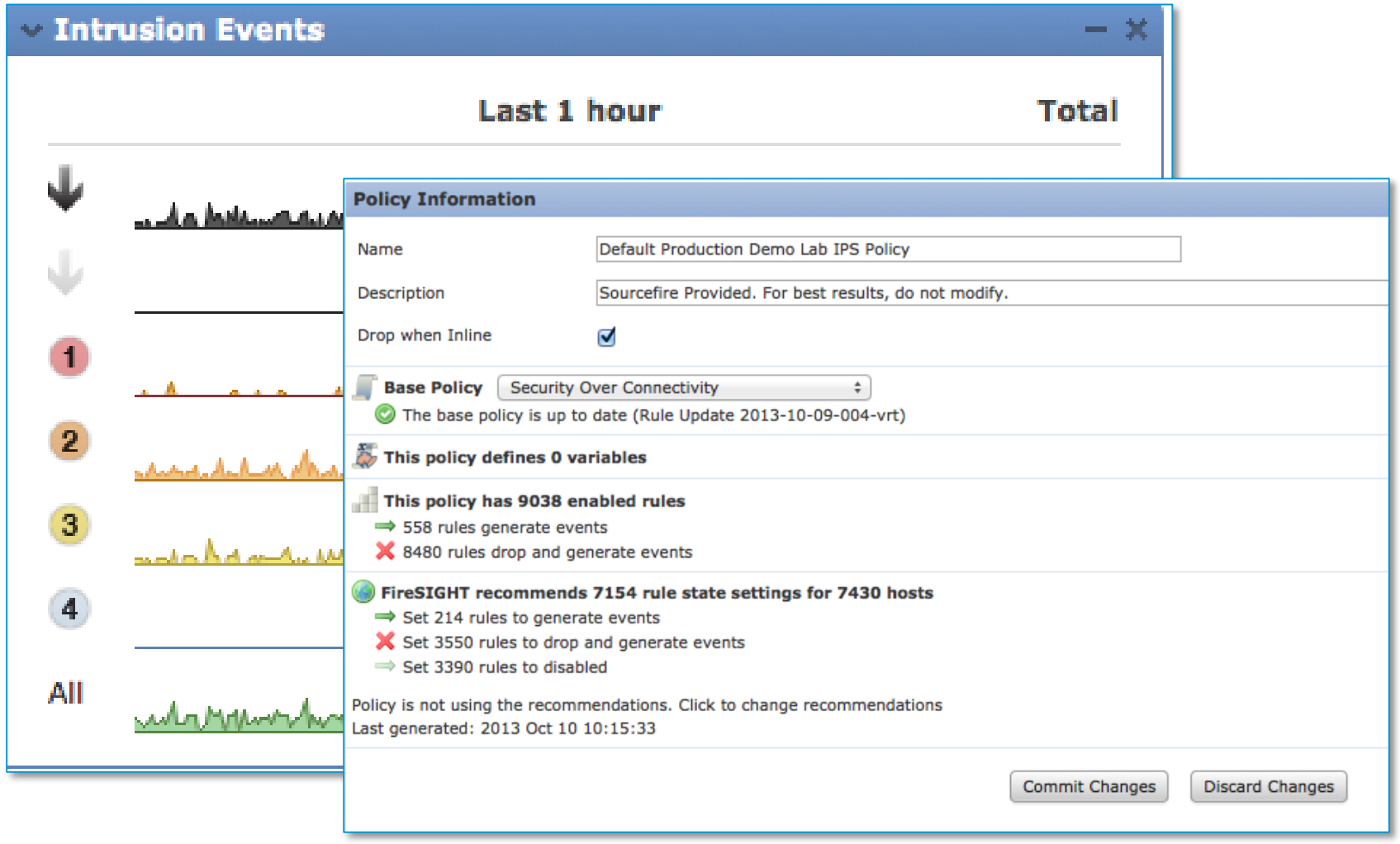

DEMO TIME!

Одна консоль – множество ролей





Автоматизация создания политик и правил



Overview | Analysis | Policies | Devices | Objects | Endpoints | Health | System | Help

Dashboards | Reporting | Summary

Report Designer

Application Statistics

Provides traffic and intrusion event statistics by application

Connections | Intrusion Events | +

Show the Last 1 hour

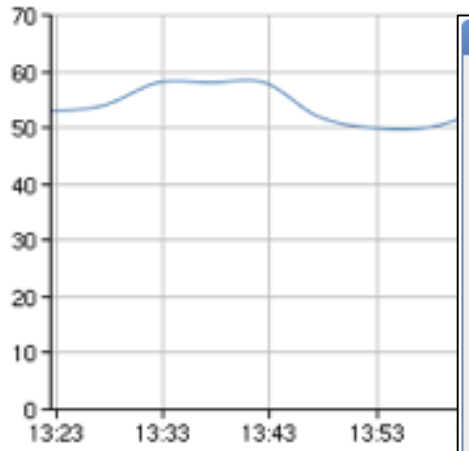
Add Widgets

Allowed Connections by Application

Application	Allowed Connections
Sun RPC	191,962
Sun RPC client	191,962
DNS	177,792
HTTP	80,881
HTTPS	41,480
+1 Direct Connect	23,586
Direct Connect	23,586
+1 SNMP	20,094
+1 Dropbox	13,369
+1 SSL	9,756

Last updated less than a minute ago

Unique Applications over Time



Last updated less than a minute ago

Risky Applications

Total Bytes (KB)
41,077.00
320.16
81.63
34.69
8.89
4.16
1.98
0.70
0.53

Allowed Connections by Business

Business Relevance	Allowed Connections
High	410,375
Medium	331,579
Very High	53,575
Very Low	6,905
Low	28

Allowed Connections by Application

Risk	Allowed
High	
Very Low	
Medium	
Very High	
Low	

Risky Applications

Title: Risky Applications
Preset: None
Table: Application Statistics
Field: Application
Aggregate: Total Bytes (KB)
Filter: High Risk Applications with Low Bu
Show: Top
Results: 10
Show Movers:
Color:

Application	Total Bytes (KB)
BitTorrent	41,077.00
eDonkey	320.16
Ustream.tv	81.63
Facebook	34.69
+1 Yet ABC	8.89
Facebook Apps	4.16
QQ	1.98
MySpace	0.70
-1 Gnutella	0.53

Last updated 4 minutes ago

ory

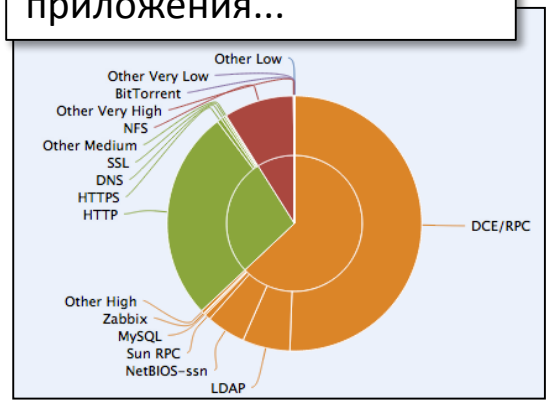
Total Traffic (KB/s)
4,412.25
3,852.30
2,721.11
1,723.48
1,354.04
404.91

Last login on Tuesday, 2011-11-15 at 10:23:56 from 10.2.100.129

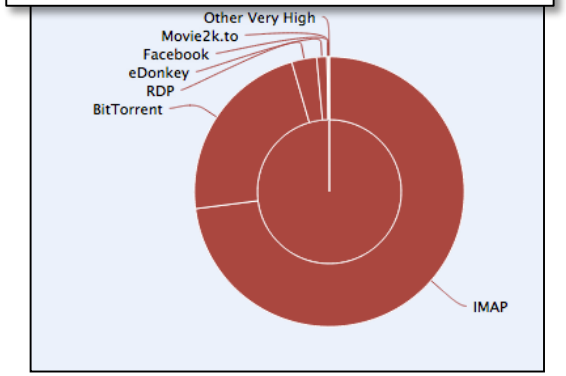
SOURCEfire

Понимание контекста в FireSIGHT

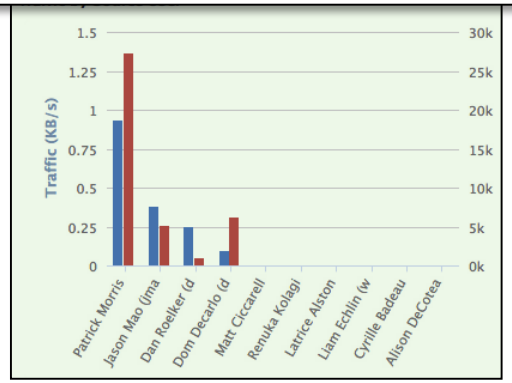
Просмотр всего трафика приложения...



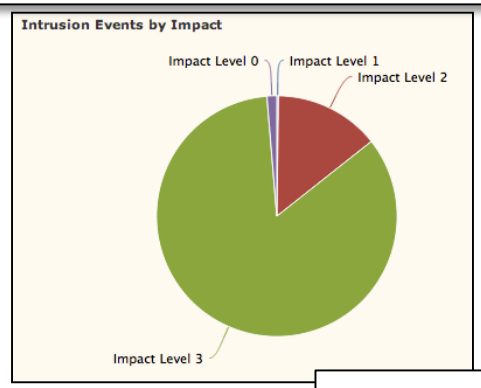
Поиск приложений с высокой степенью риска...



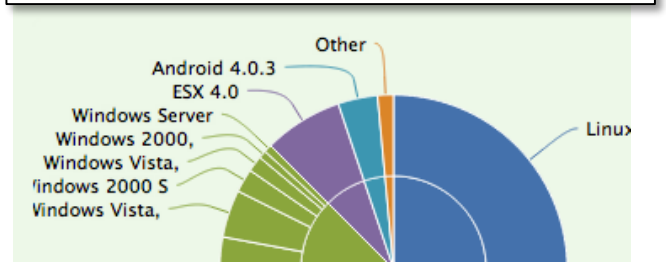
Кто их использует?



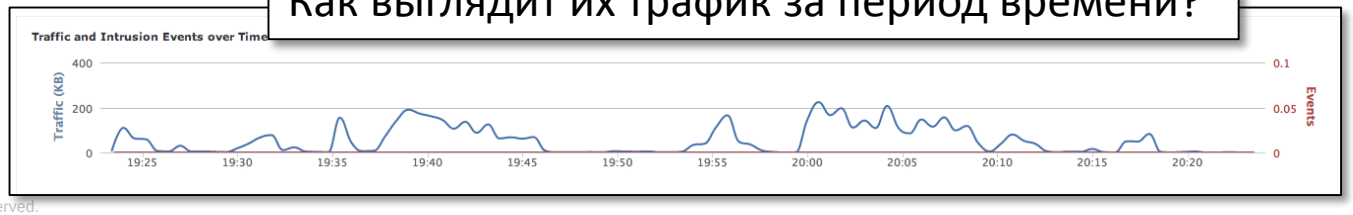
Чем еще занимались эти пользователи?



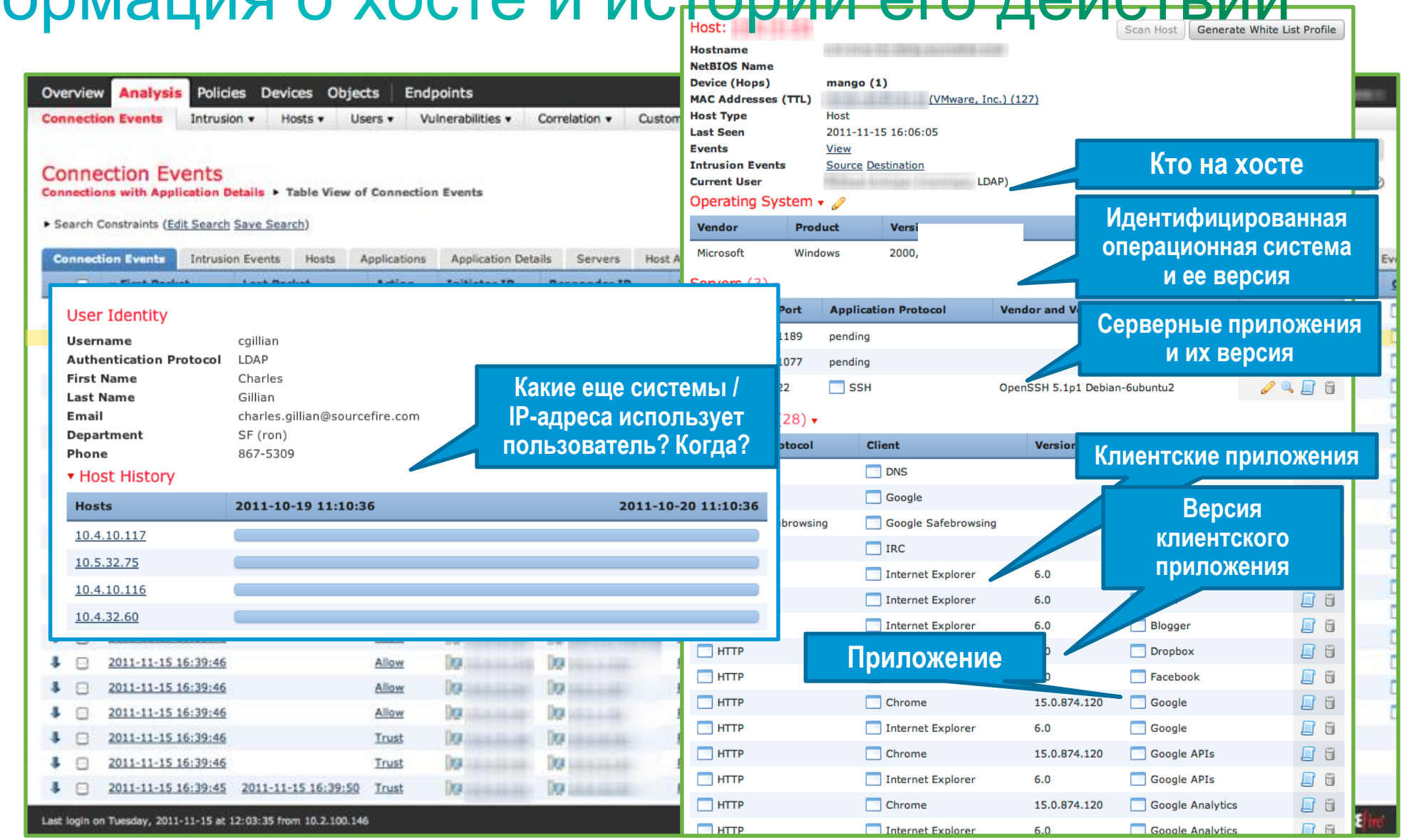
Какие использовались операционные системы?



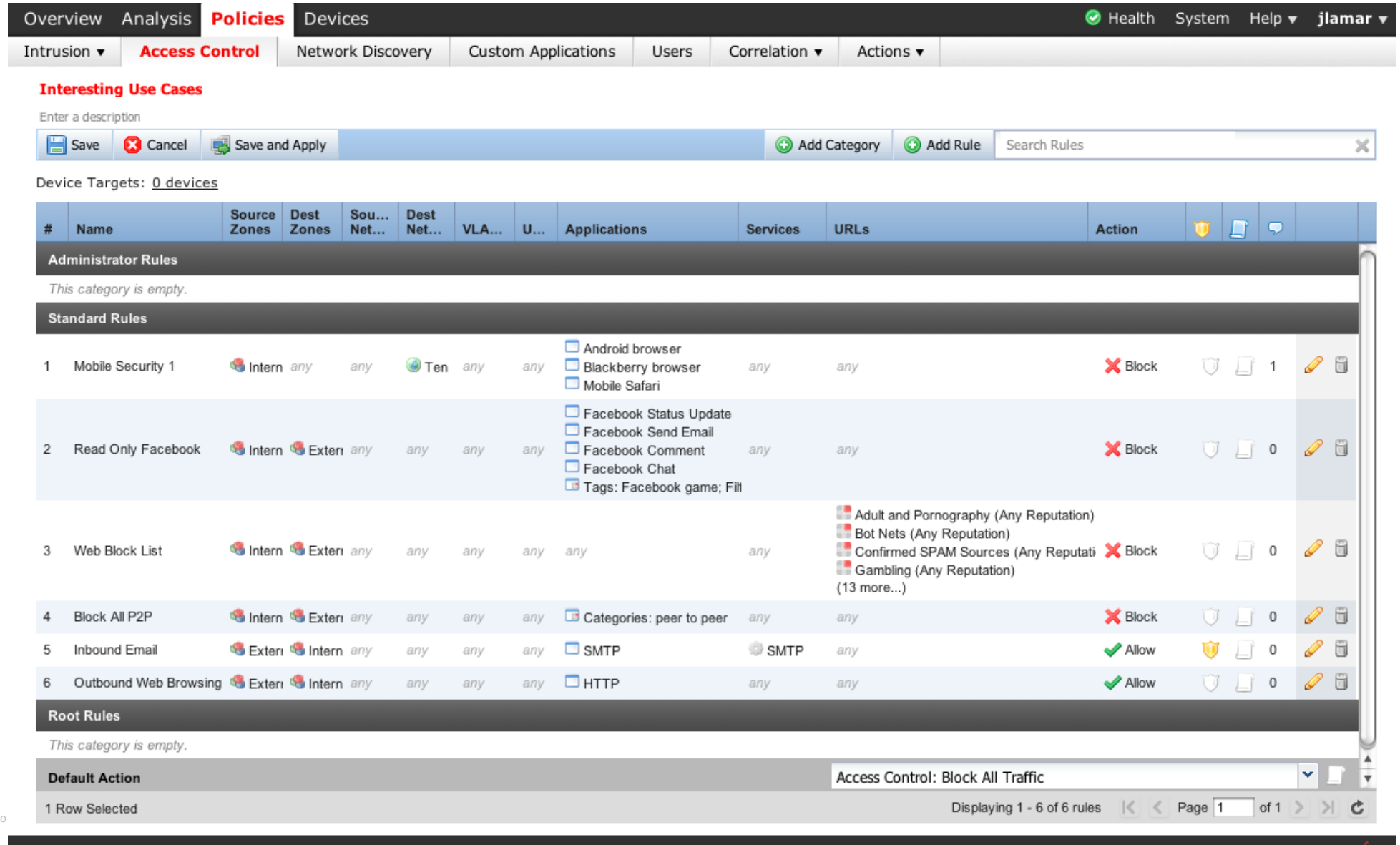
Как выглядит их трафик за период времени?



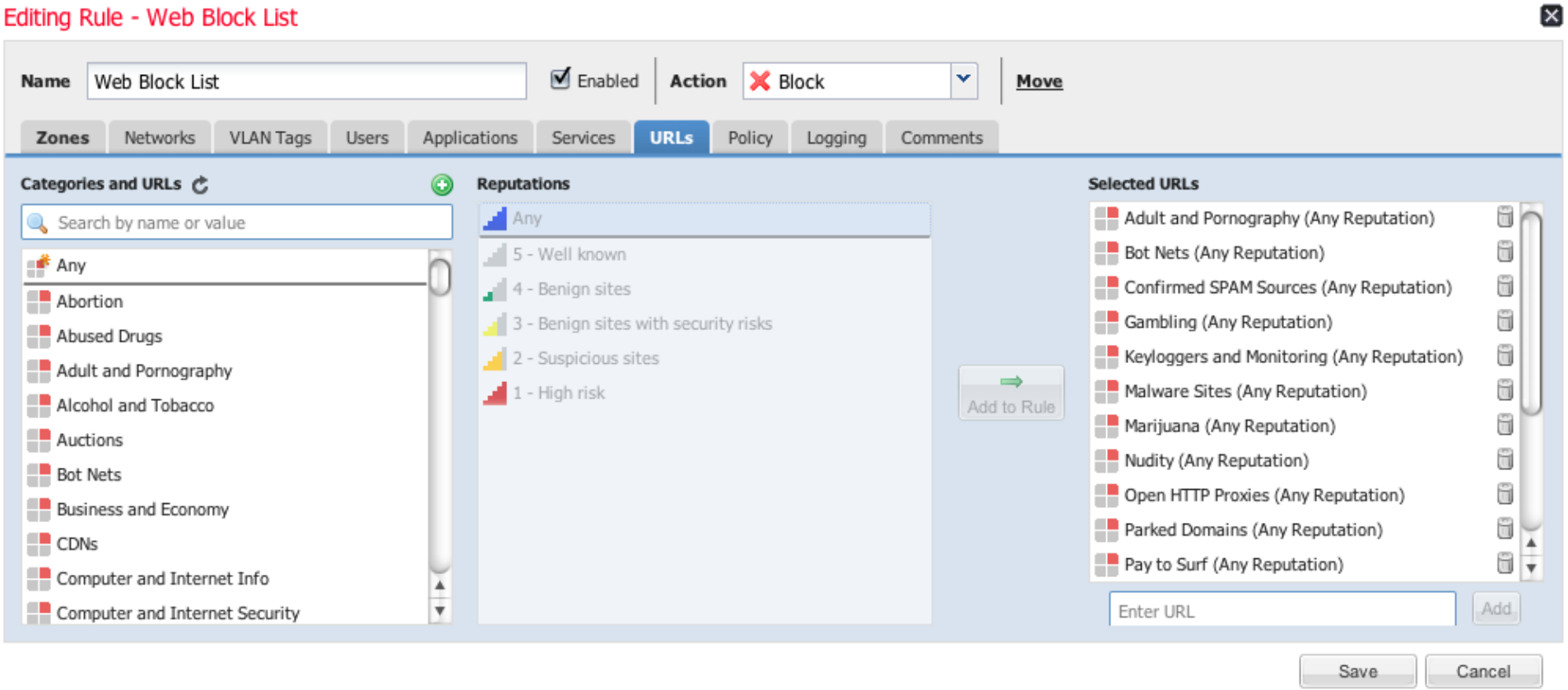
Информация о хосте и истории его действий



Управление политиками



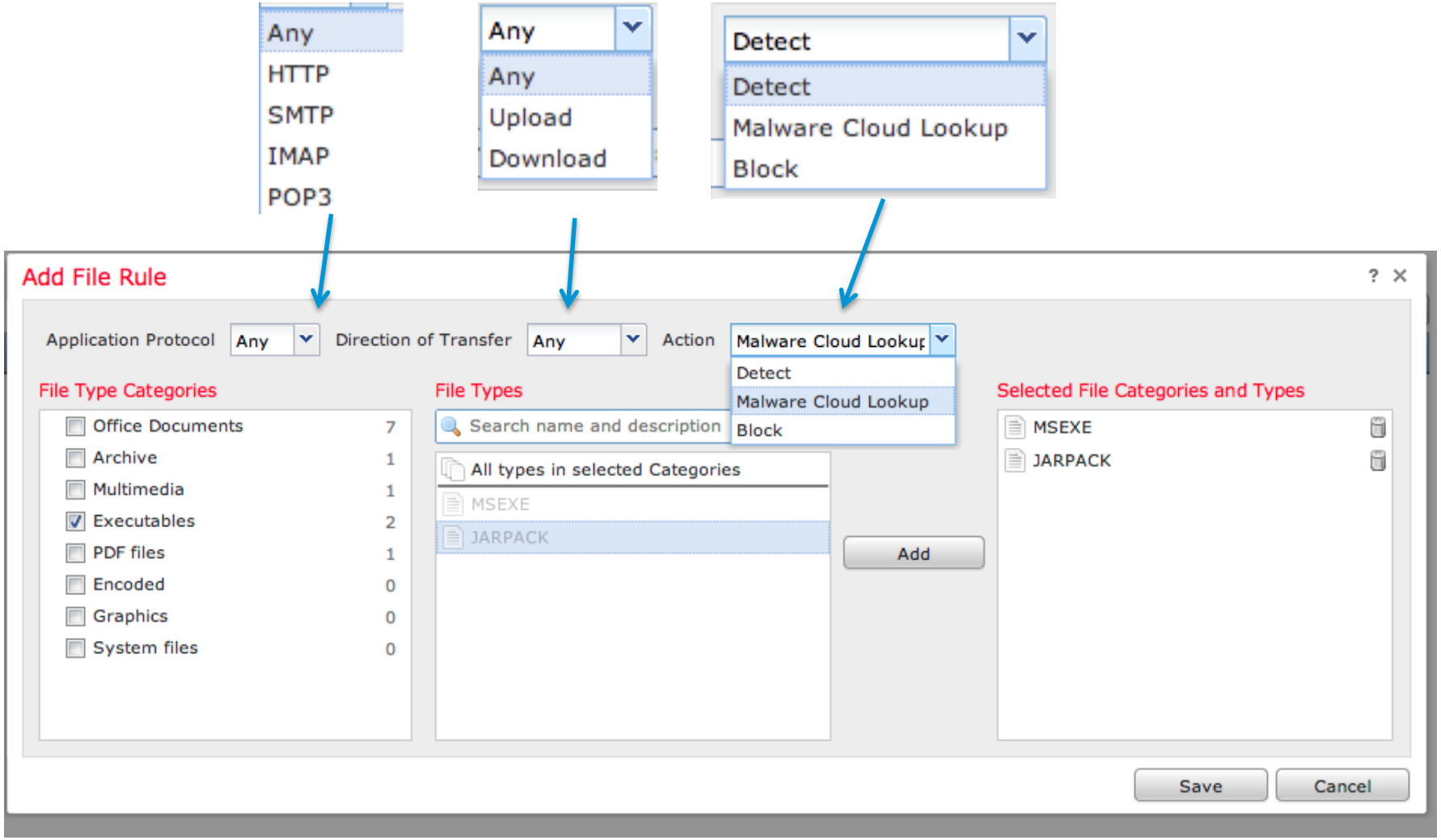
Фильтрация URL



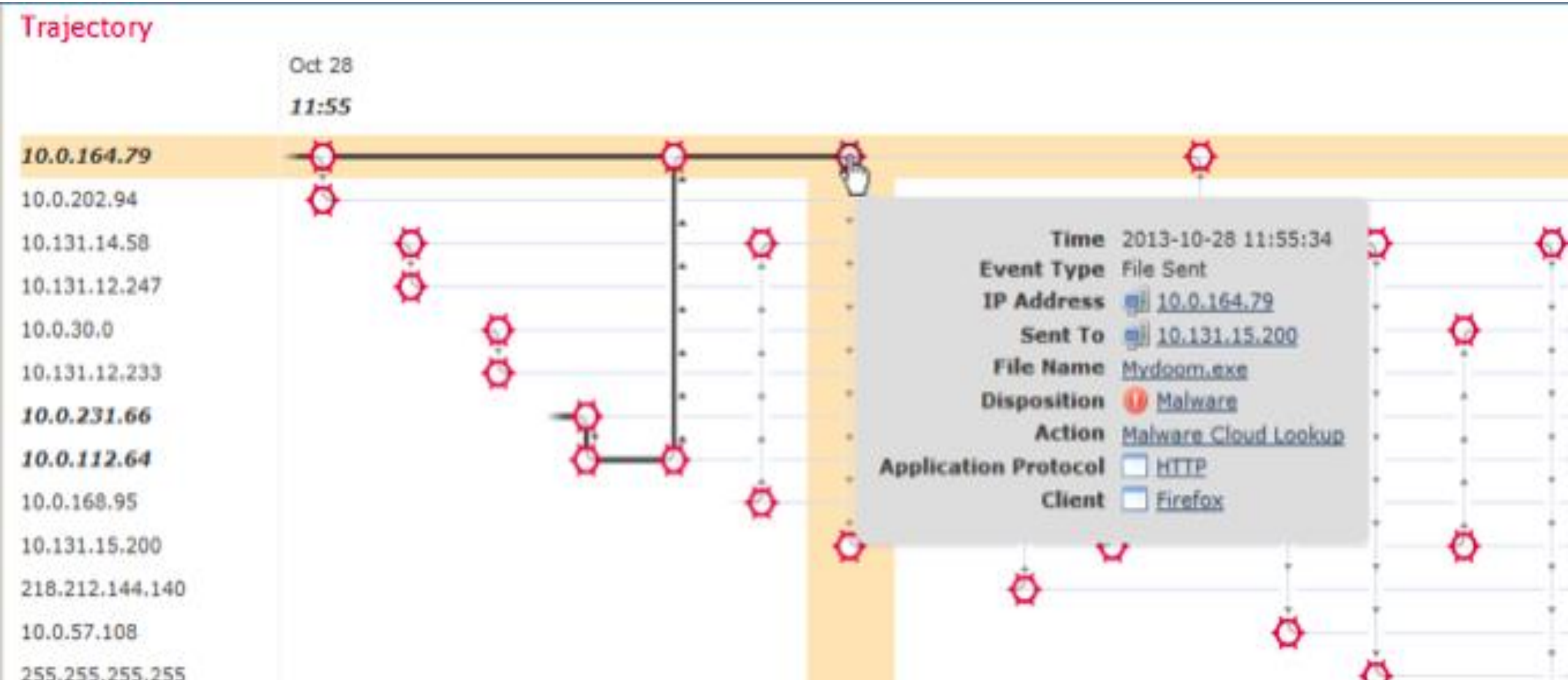
Различные категории URL

URLs категорированы по уровню рисков

Контроль по типам файлов

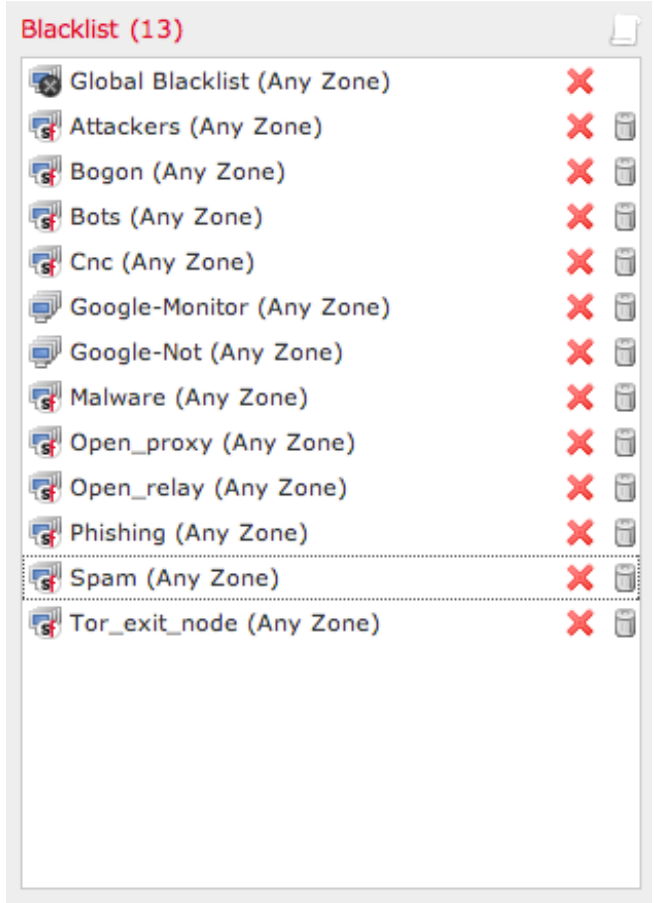


Анализ траектории файла



«Черные списки»

- **Что это?**
  - Сигналы тревоги и правила блокирования:
    - Трафик ботнетов и C&C / Известные злоумышленники / открытые прокси/релеи
    - Источники вредоносного ПО, фишинга и спама
  - Возможно создание пользовательских списков
  - Загрузка списков от Sourcefire или иных источников
- **Как это может помочь?**
  - Блокировать каналы вредоносных коммуникаций
  - Непрерывно отслеживать любые несанкционированные и новые изменения



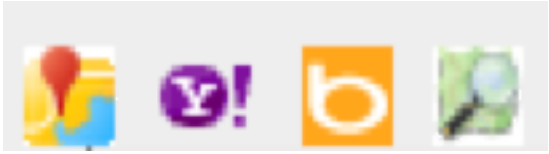
Геолокация

Top Events by Source Country

Country Name	▼ Count
United States	162
Germany	36
China	18
Japan	13
France	11
Russia	4
North Korea	2
Pakistan	1
Iraq	1
Iran	1

Last updated 1 minutes ago

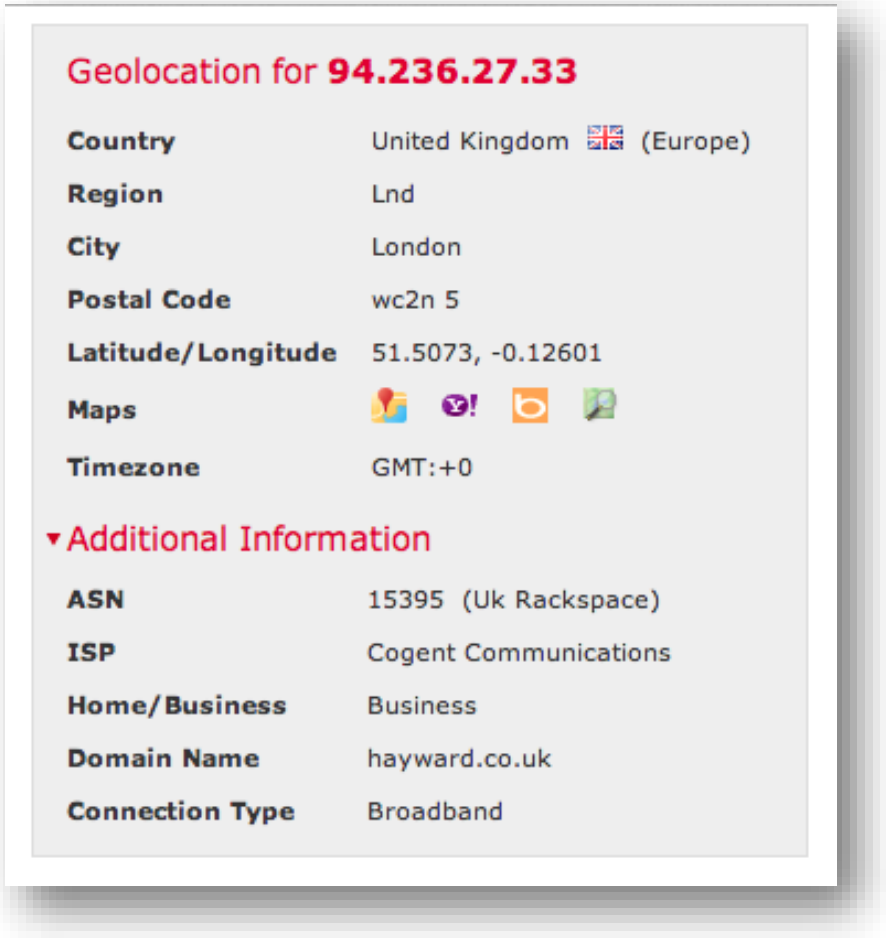
Initiator IP	Initiator Location	Responder IP
76.100.209.66	USA	10.4.32.112
10.4.10.131		10.4.32.112
10.4.10.131		10.4.32.112
10.4.33.95		10.5.32.206
89.188.101.82	ISR	10.5.32.206
200.189.215.85	BRA	10.4.33.44
10.4.31.237		10.5.32.206
10.4.11.216		10.5.39.206



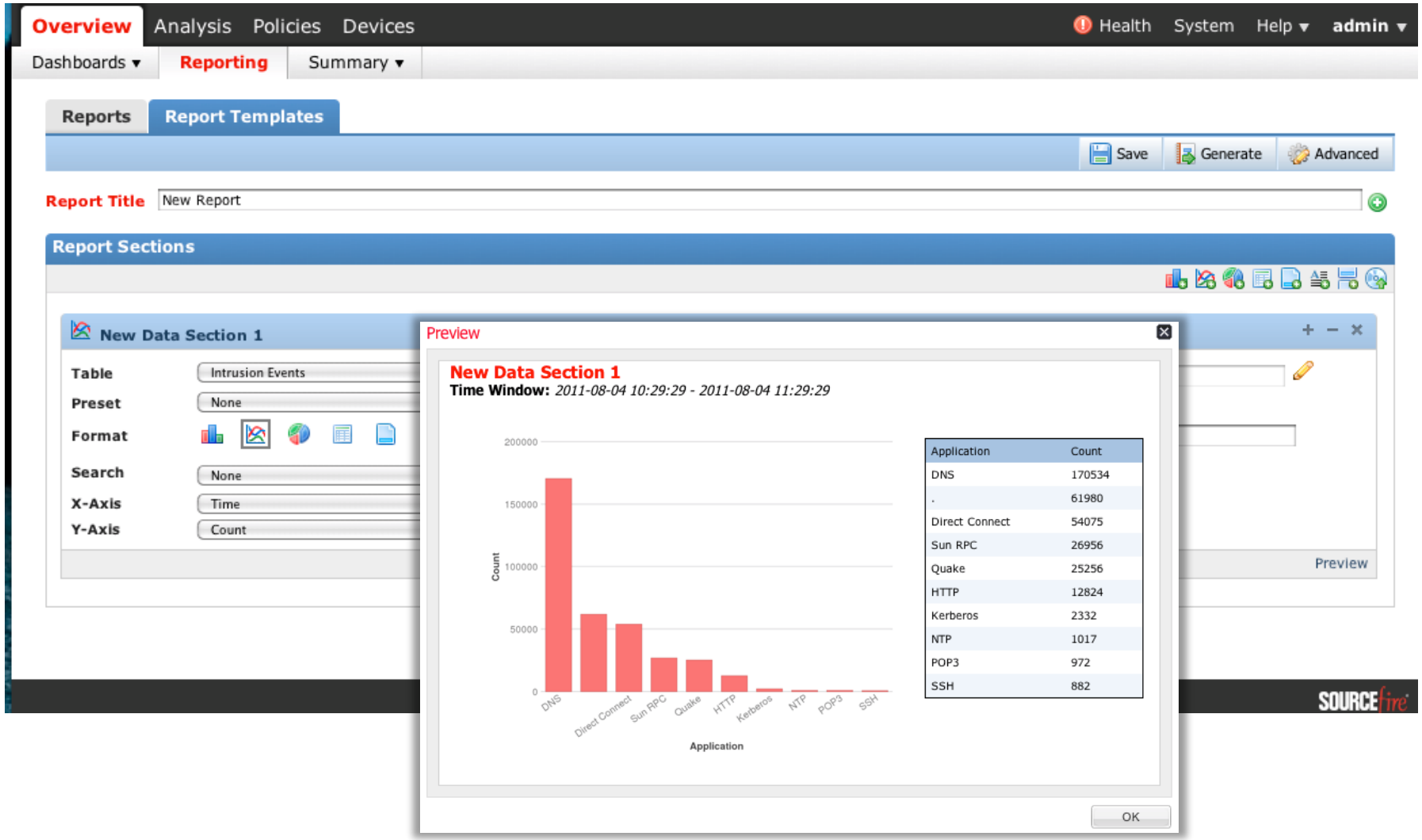
- Визуализация карт, стран и городов для событий и узлов

Детали по геолокации

- IP –адреса должны быть маршрутизируемыми
- Два типа геолокационных данных
  - Страна – включено по умолчаниют
  - Full – Может быть загружено после
  - Установки:
    - Почтовый индекс, координаты, TZ, ASN, ISP,
    - организация, доменное имя и т.д.
    - Ссылки на карты (Google, Bing и другие)
- Страна сохраняется в запись о событии
  - Для источника & получателя



Дизайнер пользовательских отчетов



Cyber Threat Defense

aka Lancope Stealthwatch

Немного фактов

- На установление факта заражения уходит в среднем 9-18 месяцев (US CERT)
  - Как правило об этом узнают от третьей стороны
- При реагировании на инцидент 75% времени тратится на поиск причины – счёт идёт на дни и недели (Forrester)
- У большинства компаний нет установленного процесса реагирования на инциденты

Как минимизировать ущерб?

Знать атакующего

Кто?	• Страна? Конкуренты? Частные лица?
Что?	• Что является целью?
Когда?	• Когда атака наиболее активна и с чем это связано?
Где?	• Где атакующие? Где они наиболее успешны?
Зачем?	• Зачем они атакуют – что конкретно их цель?
Как?	• Как они атакуют – Zero-day? Известные уязвимости? Инсайдер?

Знать себя

Кто?	• Кто в моей сети?
Что?	• Что делают пользователи? Приложения? • Что считать нормальным поведением?
Когда?	• Устройства в сети? Что считать нормальным состоянием?
Где?	• Где и откуда пользователи попадают в сеть? • Внутренние? eCommerce? Внешние?
Зачем?	• Зачем они используют конкретные приложения?
Как?	• Как всё это попадает в сеть?

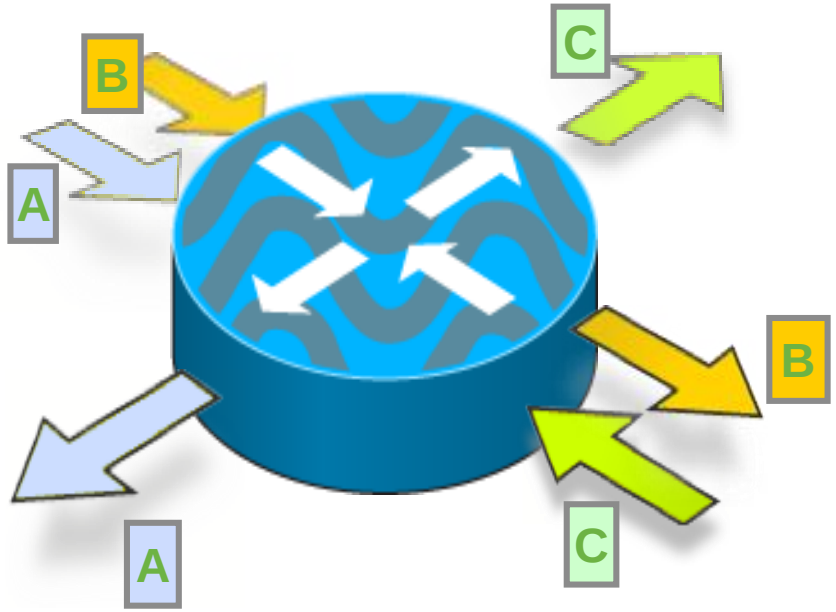
Варианты решений

Анализ сетевых потоков
- слабое воздействие на устройства
- основной инструмент исследования
- небольшой требуемый объем памяти

Система обнаружения сетевых вторжений
- на основе сигнатур
- пассивный сбор
- первичный источник оповещения

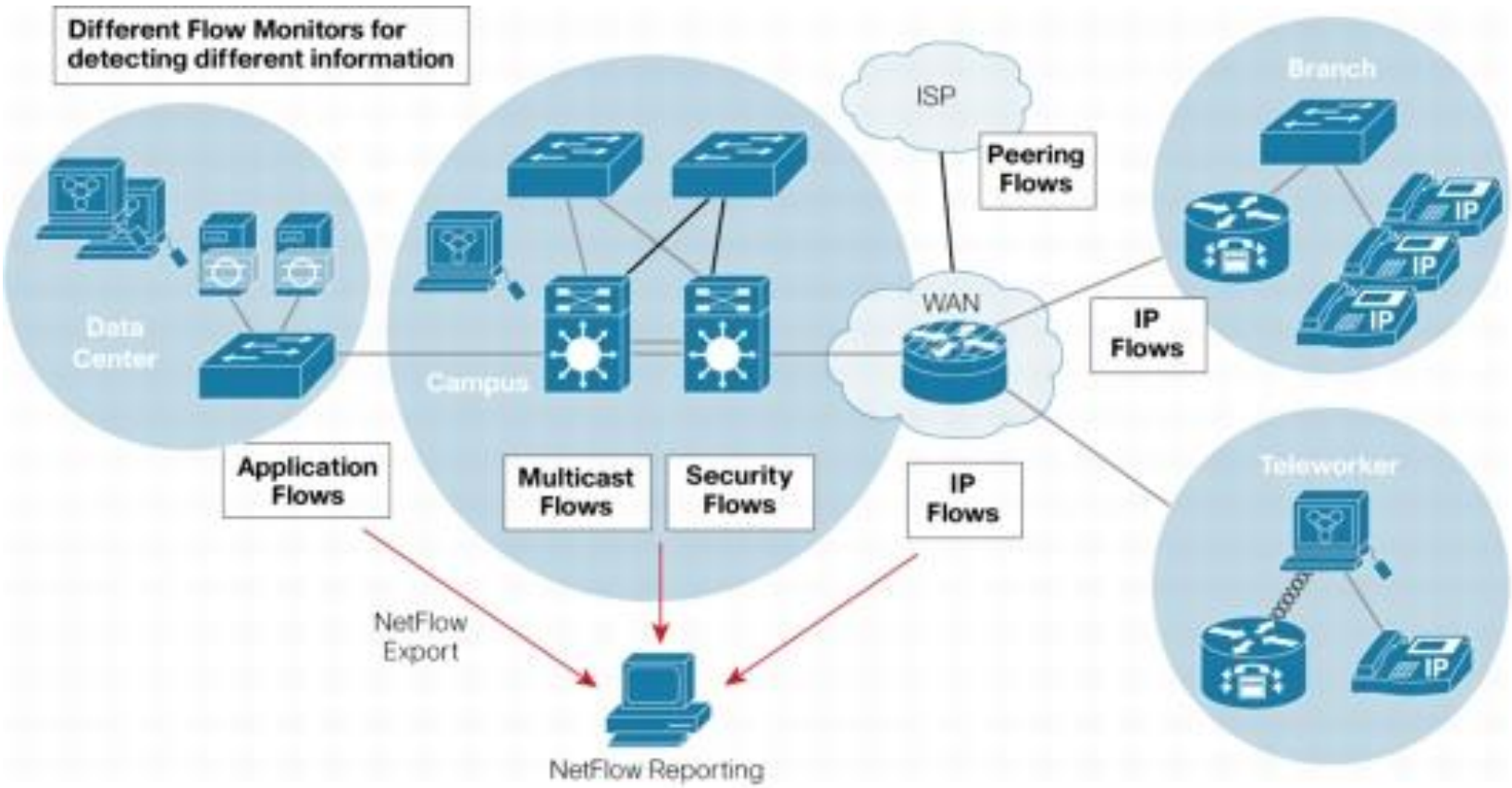
SIEM/Журнал Syslog сервера
- инструмент глубокого анализа
- возможность фильтрации
- ограниченное воздействие на систему

Не везде есть IPS, но везде есть NetFlow



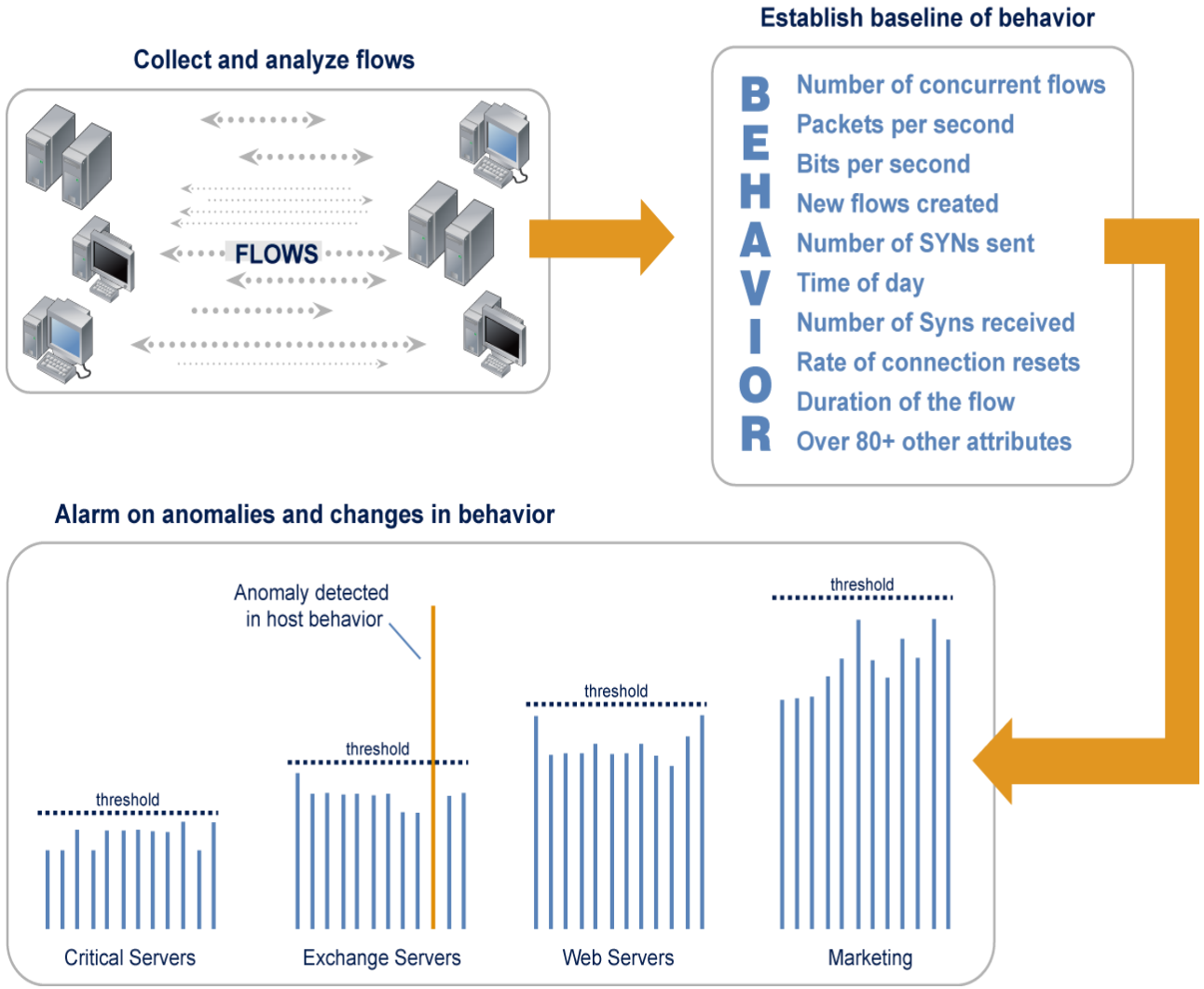
	Source IP: Port	Destination IP: Port	Packets	Date/Time
A	192.168.15.7:2068	211.160.17.195:8080	7	5/7/2009 8:11:13 GMT
B	192.168.21.5:1042	72.18.45.223:21	219	5/7/2009 9:00:03 GMT
C	192.168.6.22:3161	172.18.15.188:80	1	5/7/2009 9:05:16 GMT

Сеть как сенсор



- NetFlow можно взять из всех критичных и важных точек

Возможности CTD – Поведенческий анализ



Возможности CTD (ч.2)

- Обнаружение сетевых сканирований
- Обнаружение компьютеров-зомби и червей
- Помощь в устранении эпидемий
  - Кто нулевой пациент ?
  - С кем он контактировал ?
  - Кто из контактов заразился ?
  - Кого теперь пытаются заразить контакты ?
- Предотвращение утечек данных – превышение заданного порога по отправке данных
- Профилирование сети, инвентаризация хостов и приложений, анализ структуры трафика
- Обнаружение нелегальных серверов и P2P-трафика внутри сети

Возможности CTD (ч.3)

- Автоматическое или полуавтоматическое блокирование
  - В т.ч. на устройствах других производителей
- Сбор информации о потоках по NetFlow-like протоколам
  - NBAR, AVS, NSEL, jflow, sflow, и др.
  - В т.ч. с устройств других производителей
- Интеграция с системами SIEM, сканерами уязвимостей
- Подробнее
  - http://www.lancope.com/resource-center/partner-integration-briefs/sw-integrations/

Типы NetFlow

Sampled

- Маленькое подмножество трафика, менее 5%, собирается и используется для генерирования телеметрии. Дает покадровый обзор активности в сети, похоже на чтение книги, просматривая каждую 100-ю страницу.

Unsampled

- Телеметрия генерируется всем трафиком, при этом получается общая картина активности в сети.

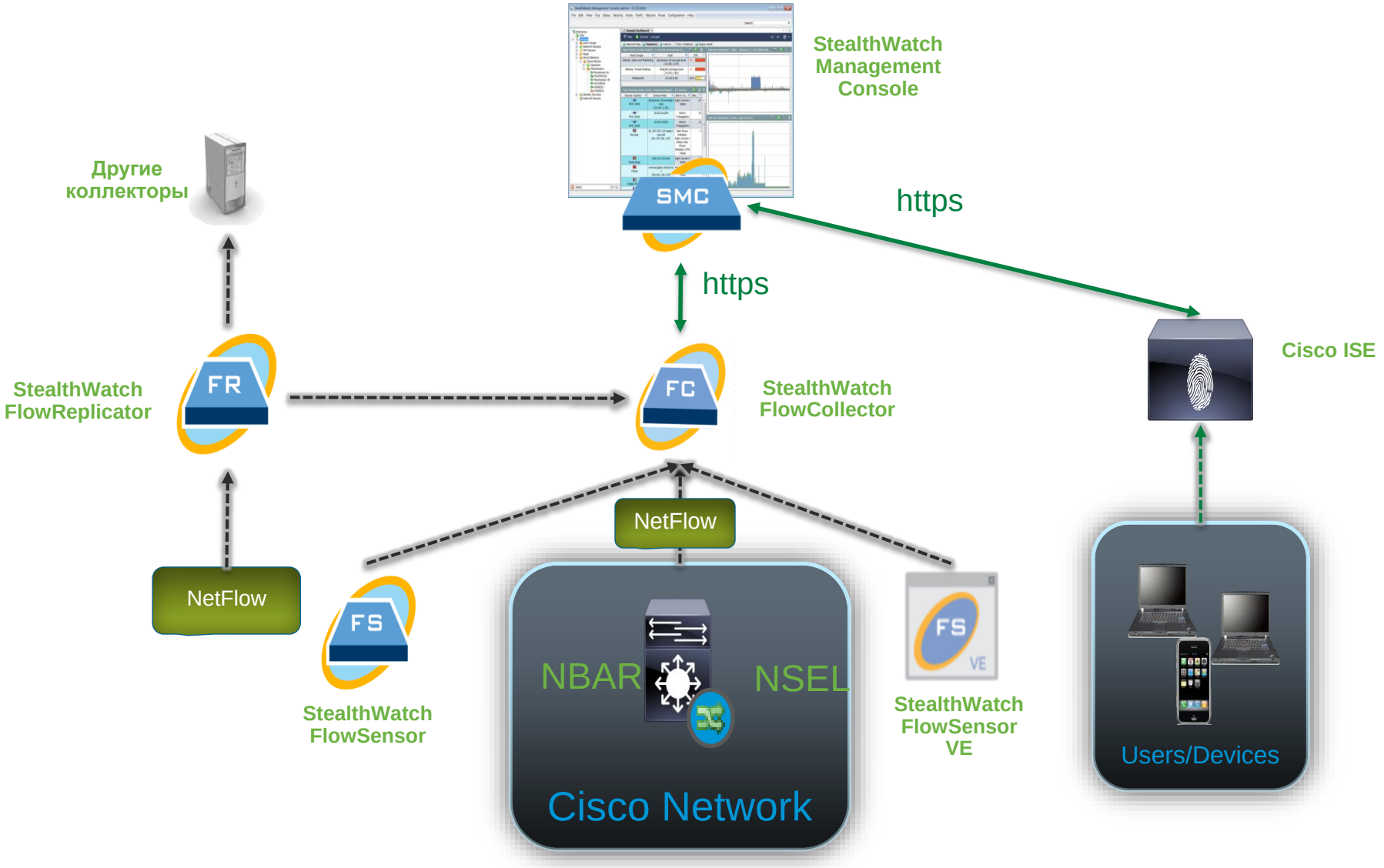
Индивидуальная, скрытая картина новых угроз требует полной информации о трафике в сети.

Только коммутаторы Cisco Catalyst могут дать информацию Unsampled NetFlow на полной скорости без влияния на производительность

Компоненты Cyber Threat Defense Solution 1.1

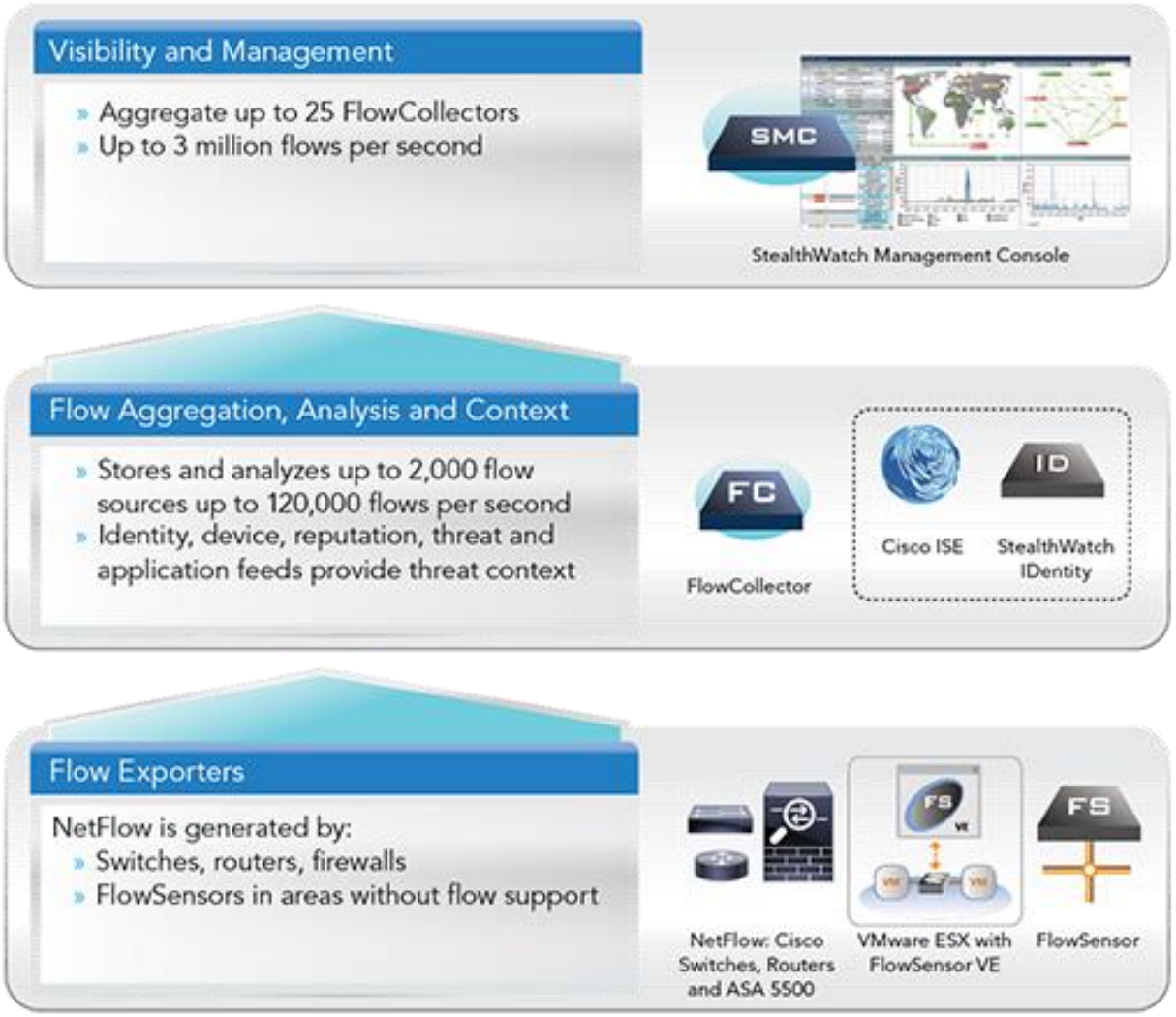
Component	Hardware	Release	Image Type and License
Catalyst 3500-X	Version ID: 02 Revision 0x03 10GE Service Module	15.0(1)SE3	Universal and IP Services
Catalyst 4500E Series	Supervisor 7E	15.0(2)X0	Universal and IP Base
	Supervisor 7L-E	15.0(2)X0	Universal and IP Base
Catalyst 6500 Series	Supervisor 2T	15.0(1)SY2	Advanced Enterprise Services, Advanced IP Services and IP Base
ISR G2	Any	15.2(4)M2	Universal and IP Base
ASR 1000	RP1/RP2	15.2(1)S or XE3.5	Universal and IP Base
Adaptive Security Appliance	Any	8.4.4(1)	Any
NetFlow Generation Appliance	3140	1.0	Any
Identity Services Engine	Any	1.1.1	Any
Lancope StealthWatch Management Console	Any	6.3	Any
Lancope StealthWatch FlowCollector	Any	6.3	Any
Lancope StealthWatch FlowSensor	Any	6.3	Any
Lancope StealthWatch FlowReplicator	Any	6.3	Any

Компоненты решения Cyber Threat Defense



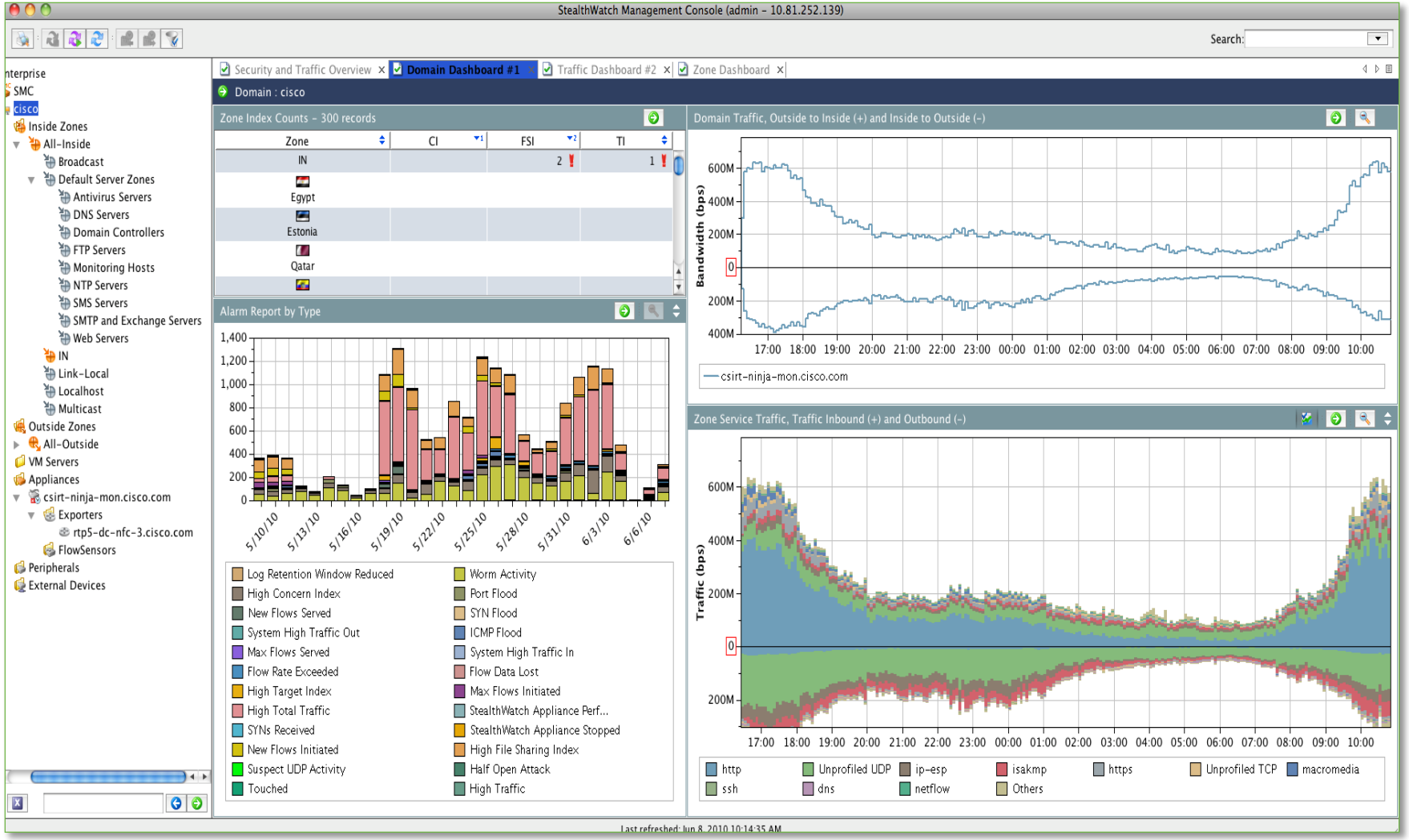
Масштабируемая архитектура

- Получение данные от сетевого оборудования с NetFlow, а также от сенсоров без поддержке NetFlow (например, VMware ESX)
- До 120.000 потоков в секунду на коллектор (до 3 миллионов на кластер)
- Понимание контекста

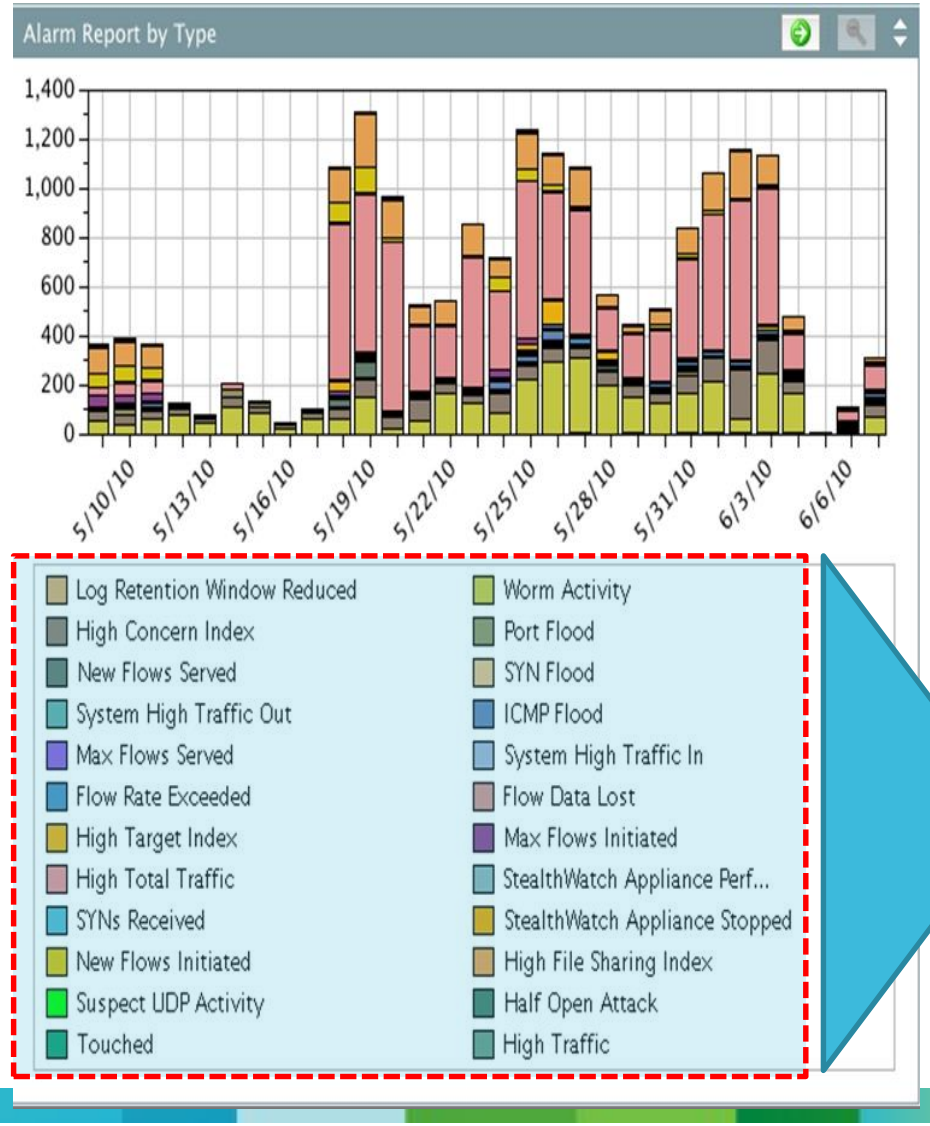



DEMO TIME!

Консоль управления CTD



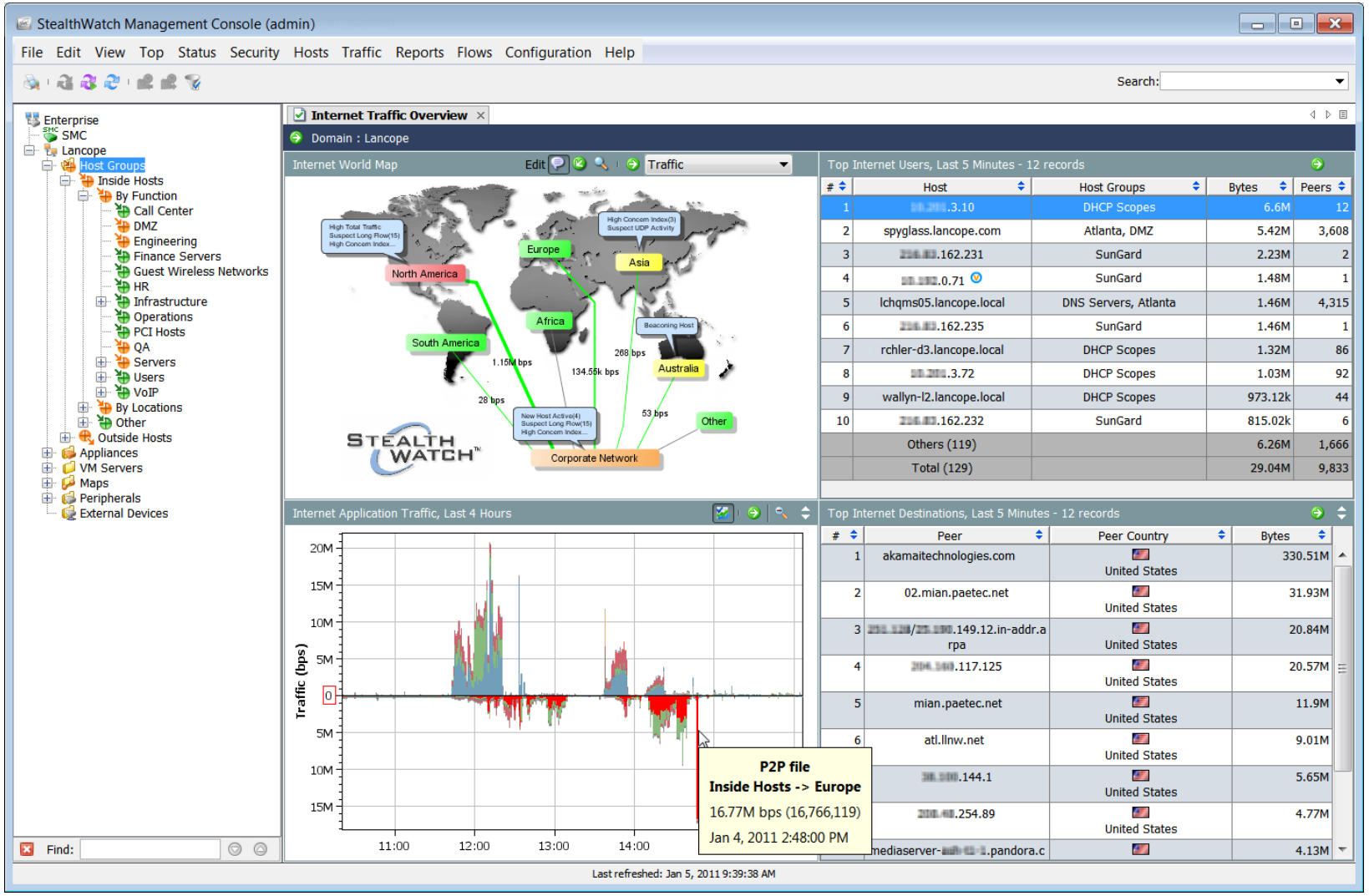
Крупным планом



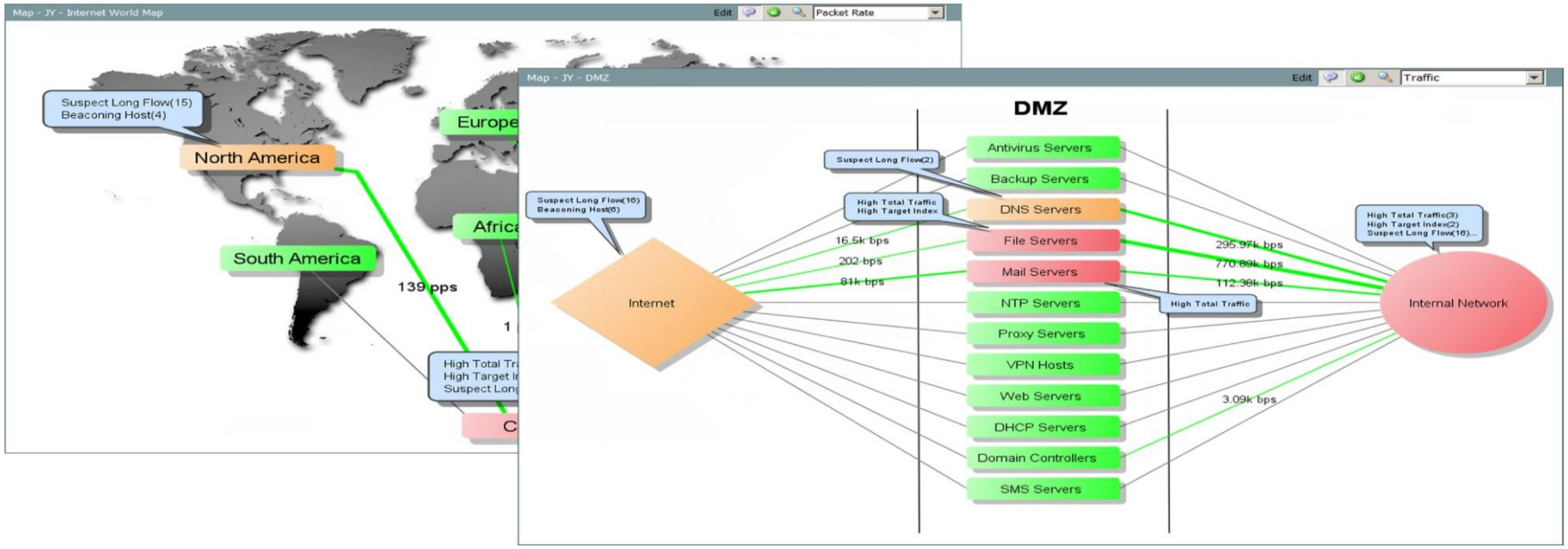
Детальная статистика о всех атаках, обнаруженных в сети

Обнаружение разных типов атак, включая DDoS

Визуализация по разным срезам

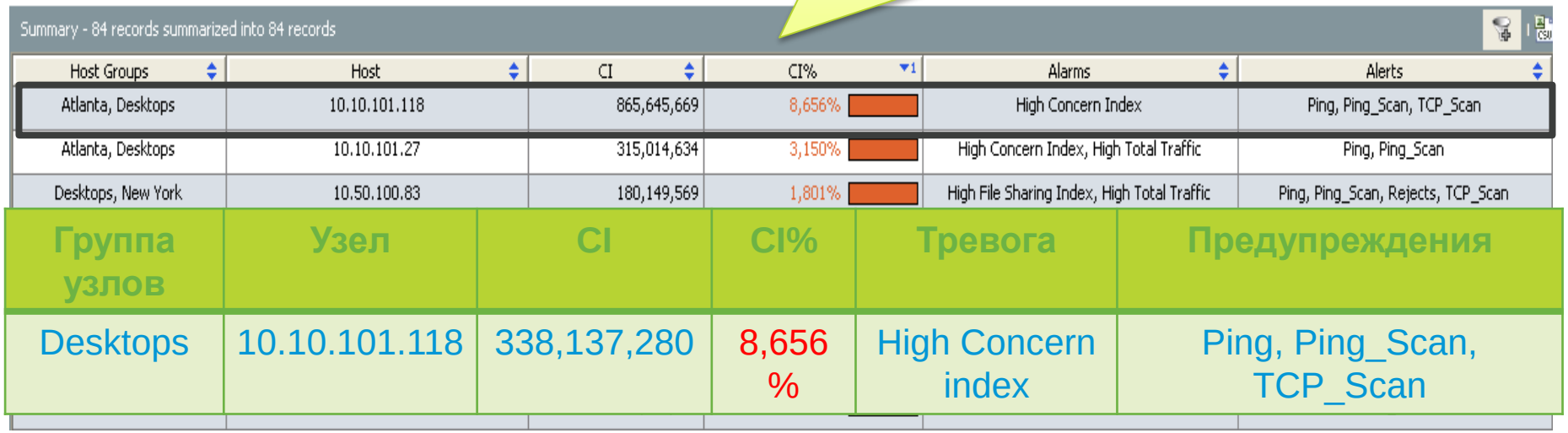


Визуализация по разным срезам



Cisco CTD: обнаружение атак без сигнатур

Высокий Concern Index показывает значительное количество подозрительных событий



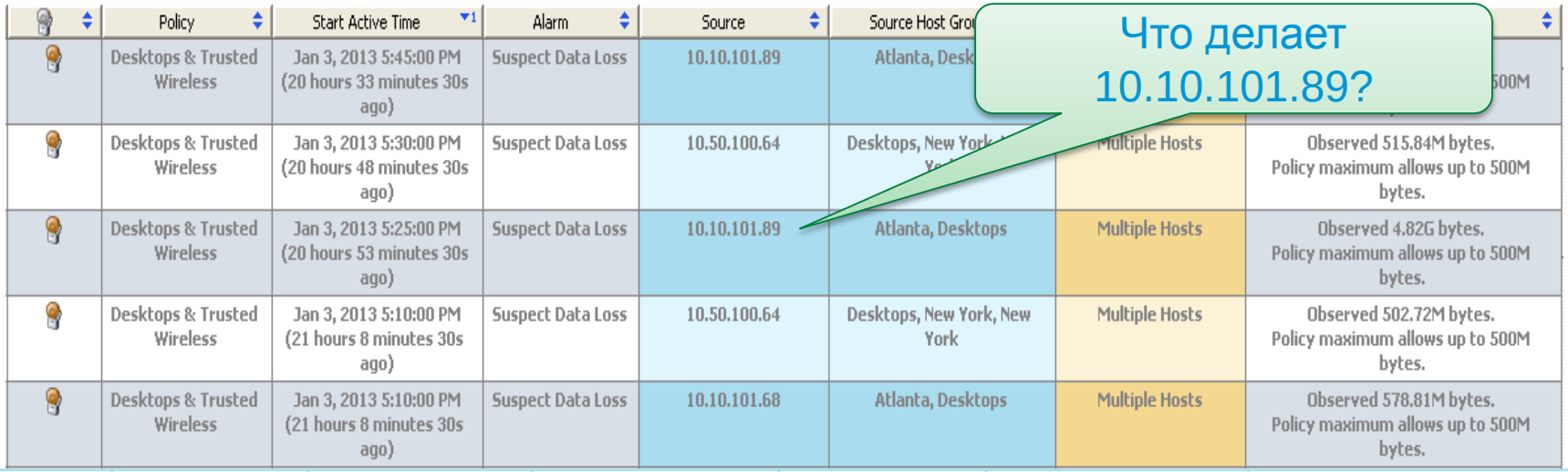
Summary - 84 records summarized into 84 records

Host Groups	Host	CI	CI%	Alarms	Alerts
Atlanta, Desktops	10.10.101.118	865,645,669	8,656%	High Concern Index	Ping, Ping_Scan, TCP_Scan
Atlanta, Desktops	10.10.101.27	315,014,634	3,150%	High Concern Index, High Total Traffic	Ping, Ping_Scan
Desktops, New York	10.50.100.83	180,149,569	1,801%	High File Sharing Index, High Total Traffic	Ping, Ping_Scan, Rejects, TCP_Scan

Группа узлов	Узел	CI	CI%	Тревога	Предупреждения
Desktops	10.10.101.118	338,137,280	8,656 %	High Concern index	Ping, Ping_Scan, TCP_Scan

Слежение за активностью как одного узла, так и группы узлов

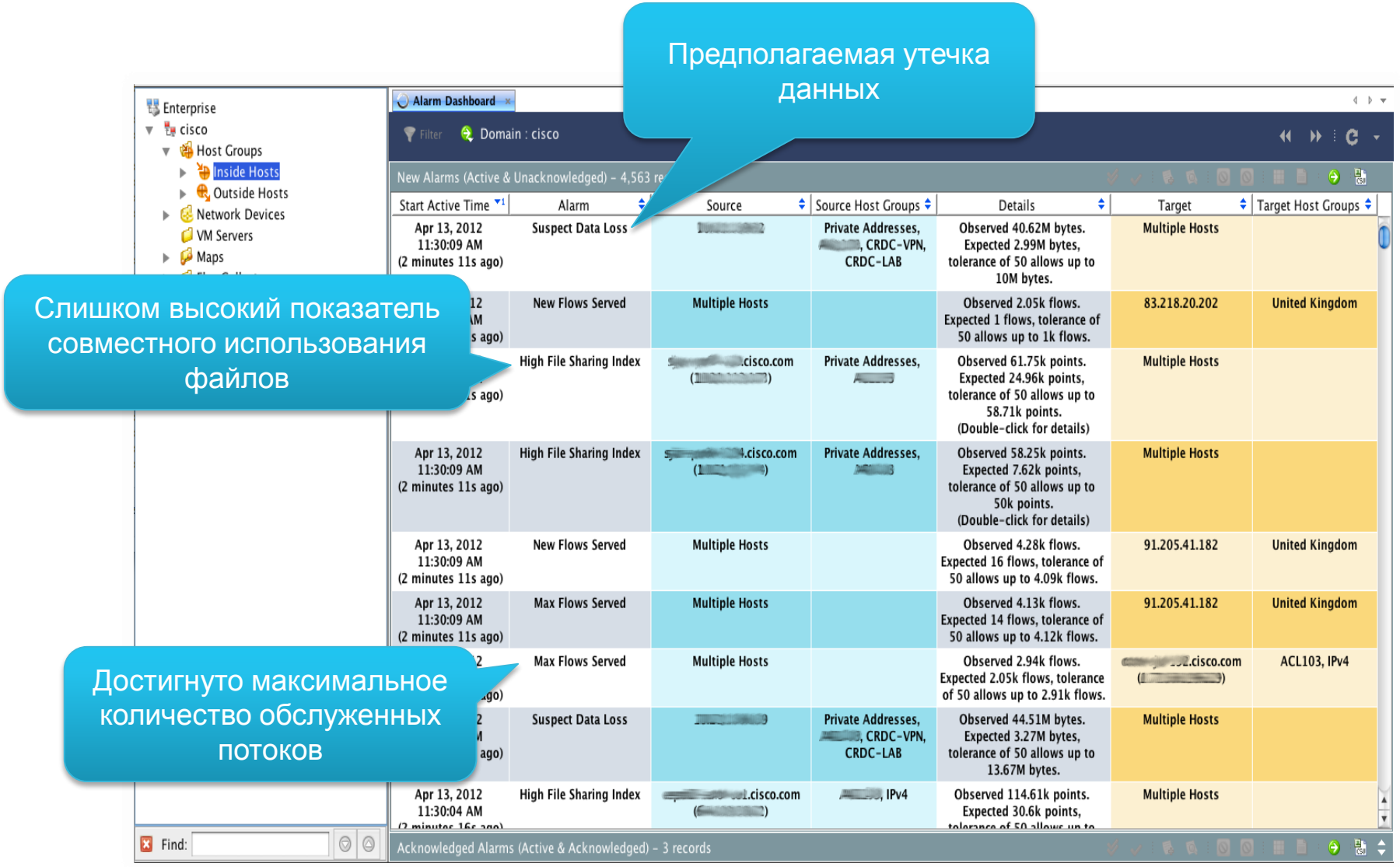
Cisco CTD: обнаружение атак без сигнатур



	Policy	Start Active Time	Alarm	Source	Source Host Gro		
	Desktops & Trusted Wireless	Jan 3, 2013 5:45:00 PM (20 hours 33 minutes 30s ago)	Suspect Data Loss	10.10.101.89	Atlanta, Desk		500M
	Desktops & Trusted Wireless	Jan 3, 2013 5:30:00 PM (20 hours 48 minutes 30s ago)	Suspect Data Loss	10.50.100.64	Desktops, New York,	Multiple Hosts	Observed 515.84M bytes. Policy maximum allows up to 500M bytes.
	Desktops & Trusted Wireless	Jan 3, 2013 5:25:00 PM (20 hours 53 minutes 30s ago)	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	Multiple Hosts	Observed 4.82G bytes. Policy maximum allows up to 500M bytes.
	Desktops & Trusted Wireless	Jan 3, 2013 5:10:00 PM (21 hours 8 minutes 30s ago)	Suspect Data Loss	10.50.100.64	Desktops, New York, New York	Multiple Hosts	Observed 502.72M bytes. Policy maximum allows up to 500M bytes.
	Desktops & Trusted Wireless	Jan 3, 2013 5:10:00 PM (21 hours 8 minutes 30s ago)	Suspect Data Loss	10.10.101.68	Atlanta, Desktops	Multiple Hosts	Observed 578.81M bytes. Policy maximum allows up to 500M bytes.

Политика	Время начала	Тревога	Источник	Source Host Groups	Цель	Детали
Desktops & Trusted Wireless	Янв 3, 2013	Вероятная утечка данных	10.10.101.89	Атланта, Десктопы	Множество хостов	Наблюдается 5.33 Гб. Политика позволяет максимум до 500 Мб

Предустановленные политики



Получение контекста от Cisco ISE

Policy	Start Active Time	Alarm	Source	Source Host Groups	Source User ...	Source Devic...	Target	Details
Desktops & Trusted Wireless	Jan 3, 2013 5:45:00 PM (20 hours 33 minutes 30s ago)	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	ud0158	Windows7-Workstation	Multiple Hosts	Observed 5.33G bytes. Policy maximum allows up to 500M bytes.
Desktops & Trusted Wireless	Jan 3, 2013 5:30:00 PM (20 hours 48 minutes 30s ago)	Suspect Data Loss	10.50.100.64	Desktops, New York, New York	ud0142	Apple-iPad	Multiple Hosts	Observed 515.84M bytes. Policy maximum allows up to 500M bytes.
Desktops & Trusted Wireless	Jan 3, 2013 5:25:00 PM (20 hours 53 minutes 30s ago)	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	ud0158	Windows7-Workstation	Multiple Hosts	Observed 4.82G bytes. Policy maximum allows up to 500M bytes.
Desktops & Trusted Wireless	Jan 3, 2013 5:10:00 PM (21 hours 8 minutes 30s ago)	Suspect Data Loss	10.50.100.64	Desktops, New York, New York	ud0142	Apple-iPad	Multiple Hosts	Observed 502.72M bytes. Policy maximum allows up to 500M bytes.
Desktops & Trusted Wireless	Jan 3, 2013 5:10:00 PM (21 hours 8 minutes	Suspect Data Loss	10.10.101.68	Atlanta, Desktops	uc0123r	Windows7-Workstation	Multiple Hosts	Observed 578.81M bytes. Policy maximum allows up to 500M

Политика	Время старта	Тревога	Источник	Группа хостов источника	Имя пользователя	Тип устройства	Цель
Desktops & Trusted Wireless	Янв 3, 2013	Вероятная утечка данных	10.10.101.89	Атланта, Десктопы	Джон Смит	Apple-iPad	Множество хостов

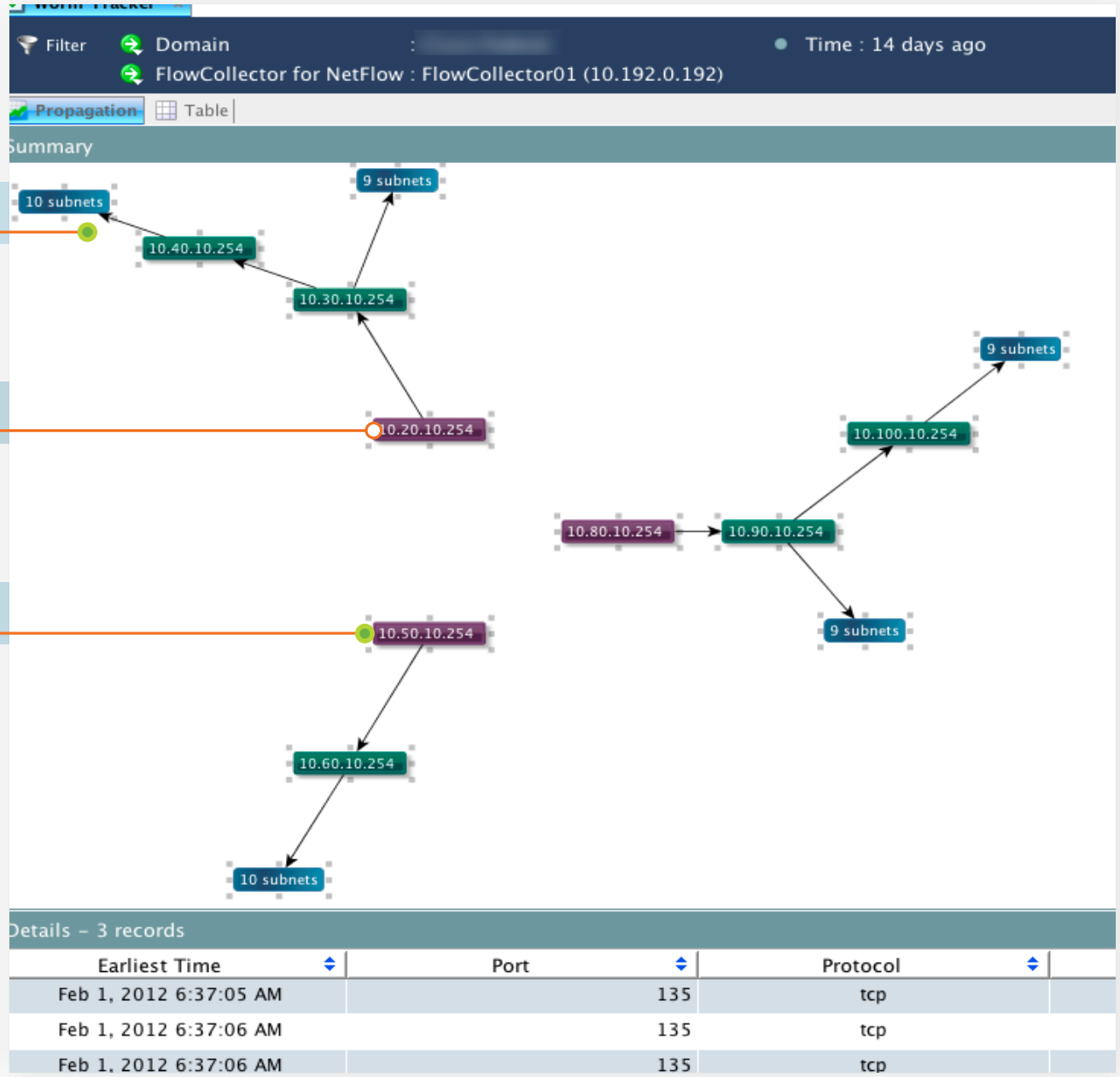
- Cisco ISE установлен в 1/3 всех проектов по Cisco Threat Defense (CTD)

Карта эпидемии

Третичное заражение

Вторичное заражение

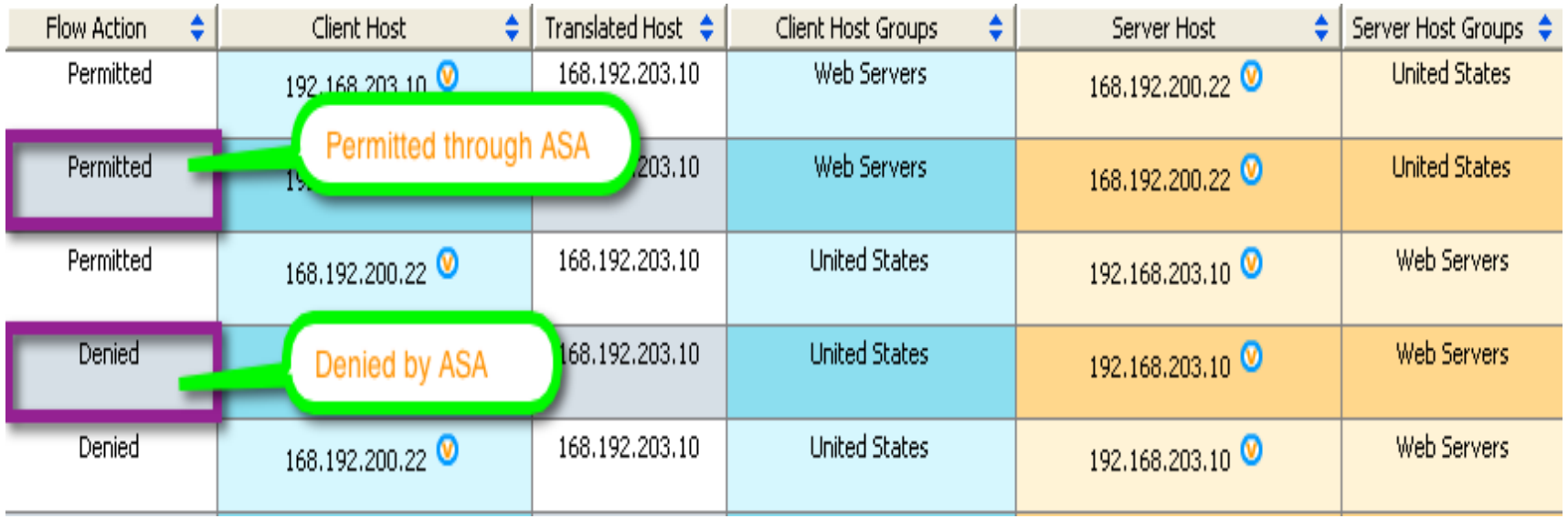
«Нулевой пациент»



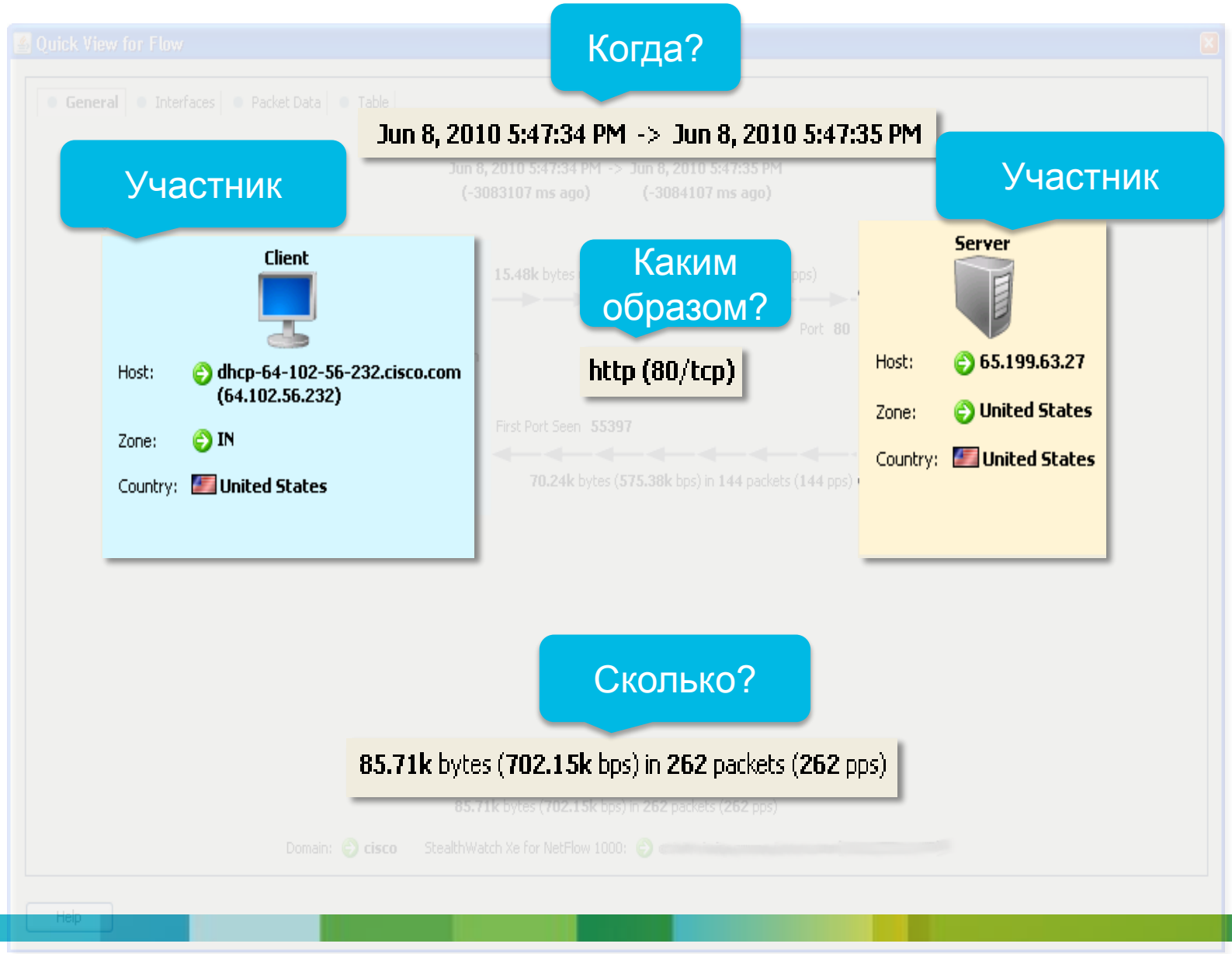
Получение контекста от Cisco ASA / ISR / ASR

- Поле Flow Action может добавить дополнительный контекст
- NSEL-отчетность на основе состояний для поведенческого анализа

  Сбор информации о отклоненных или разрешенных соединениях



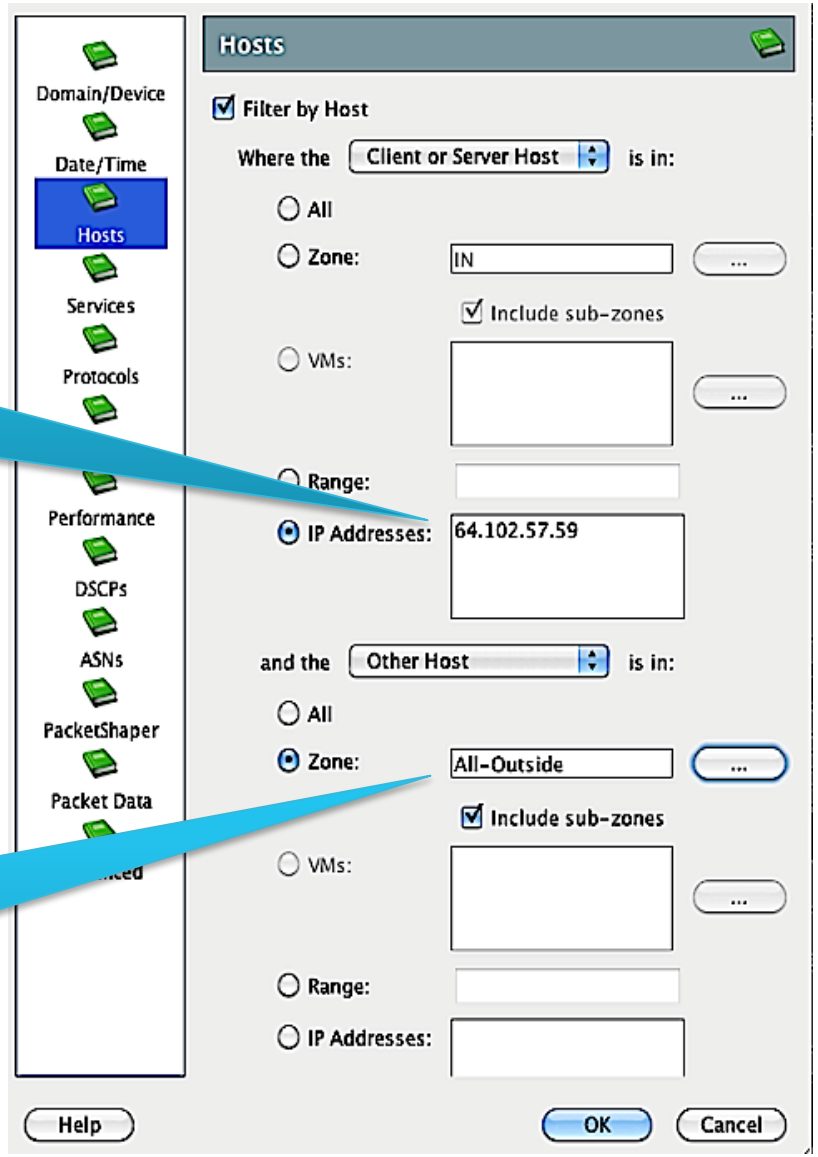
Расследование инцидентов



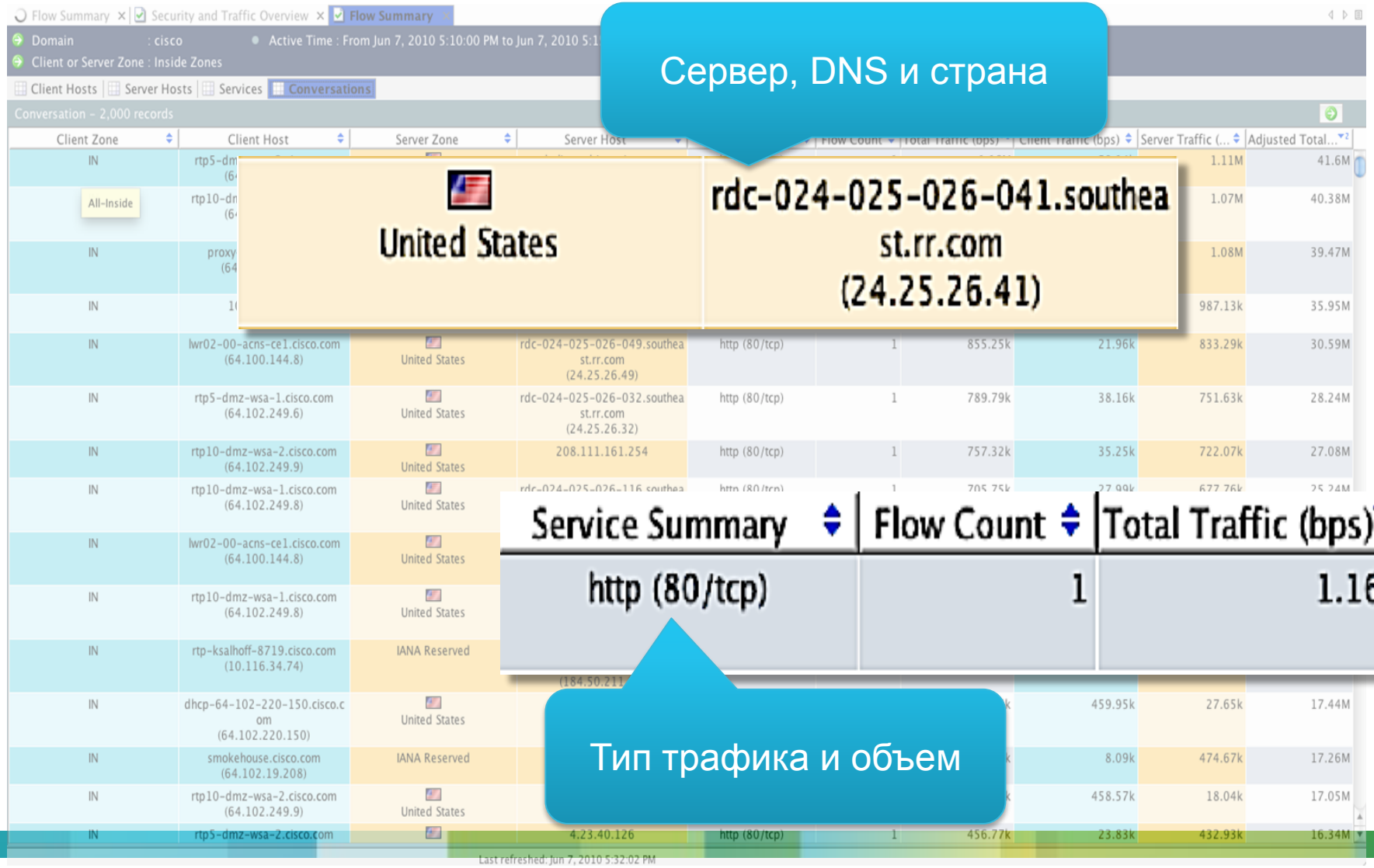
Запрос интересующей информации

Выберите узел для исследования

Поиск исходящего трафика



Результаты запроса



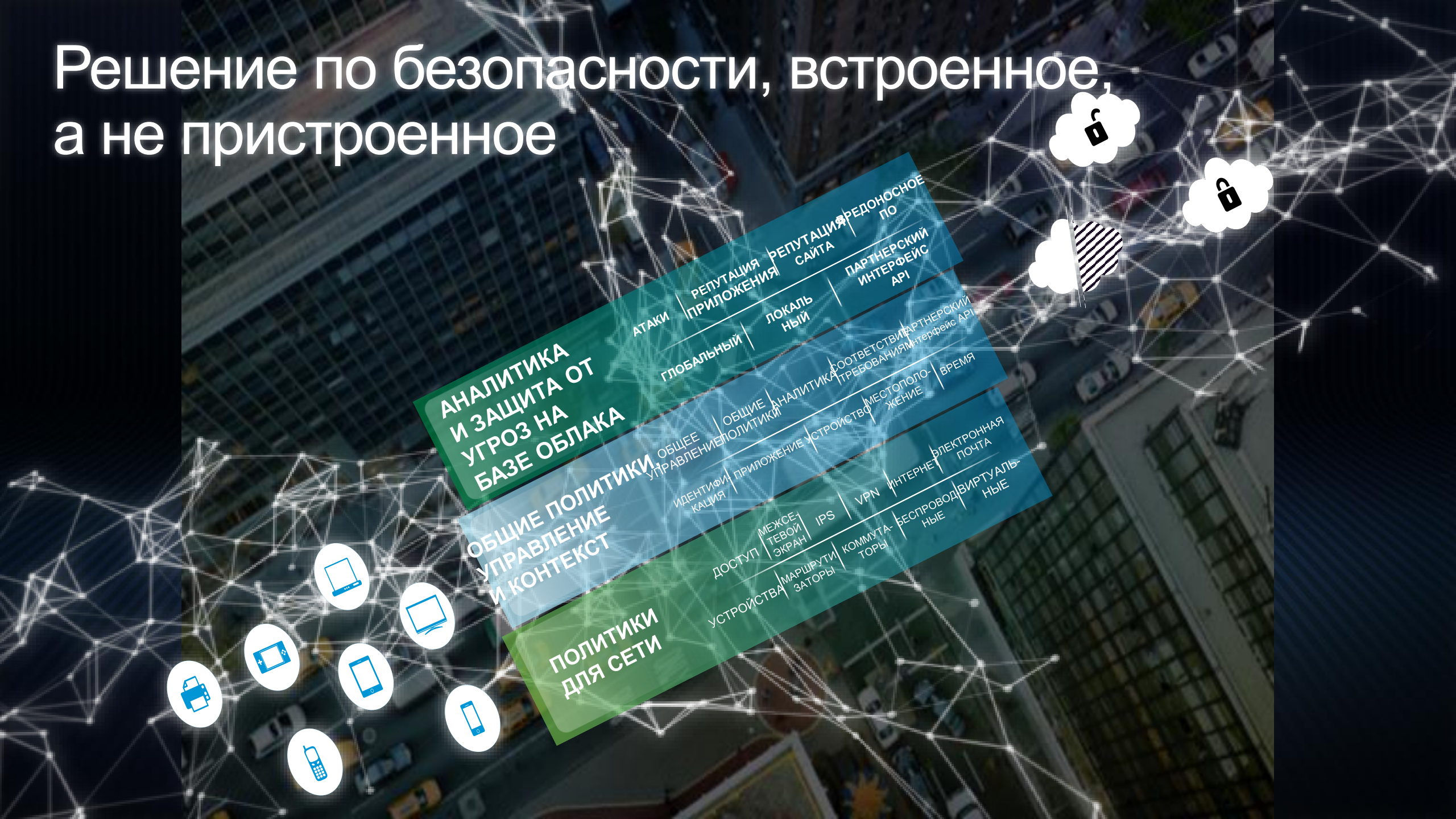
Начните с пилотного внедрения

- Оба решения доступны в виде ВМ и имеют временные лицензии
- Не требуют изменений в сети, только зеркальную копию трафика и NetFlow
- Разворачиваются в течение нескольких дней-недели
- Приносят ощутимые результаты
  - Обнаружение компьютеров-зомби и червей
  - Профилирование трафика и приложений
  - Инвентаризация хостов
  - Обнаружение нелегальных серверов и P2P-трафика внутри сети

Спасибо!

amoskvit@cisco.com

Решение по безопасности, встроенное, а не пристроенное



Sourcefire FireSIGHT «видит все»

КАТЕГОРИИ	ПРИМЕРЫ	SOURCEFIRE СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ И МЕЖСЕТВЫЕ ЭКРАНЫ НОВОГО ПОКОЛЕНИЯ	СТАНДАРТНАЯ СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ	СТАНДАРТНЫЙ МЕЖСЕТЕВОЙ ЭКРАН НОВОГО ПОКОЛЕНИЯ
Угрозы	Атаки, аномалии	✓	✓	✓
Пользователи	AD, LDAP, POP3	✓	✗	✓
Веб-приложения	Facebook Chat, Ebay	✓	✗	✓
Протоколы приложений	HTTP, SMTP, SSH	✓	✗	✓
Передача файлов	PDF, Office, EXE, JAR	✓	✗	✓
Вредоносное ПО	Conficker, Flame	✓	✗	✗
Серверы C&C	Интеллектуальная система безопасности C&C	✓	✗	✗
Клиентские приложения	Firefox, IE6, BitTorrent	✓	✗	✗
Веб-серверы	Apache 2.3.1, IIS4	✓	✗	✗
Операционные системы	Windows, Linux	✓	✗	✗
Маршрутизаторы и коммутаторы	Cisco, Nortel, Wireless	✓	✗	✗
Мобильные устройства	iPhone, Android, Jail	✓	✗	✗
Принтеры	HP, Xerox, Canon	✓	✗	✗
VoIP-телефоны	Avaya, Polycom	✓	✗	✗
Виртуальные машины	VMware, Xen, RHEV	✓	✗	✗

Next-Gen FW (NGFW)

Стандартные возможности «предыдущего поколения»

Понимание приложений и их компонентов

Встроенный сетевой IPS

Интеграция с внешними сервисами, пример:

- Каталоги пользователей
- «Репутационные» сервисы

Next-Gen IPS (NGIPS)

Стандартные возможности «предыдущего поколения»

Понимание приложений

Понимание контекста и контента

Гибкий движок, оперативные обновления сигнатур

“NGIPS в будущем войдёт в NGFW, но сейчас большинство существующих NGFW обладают только базовым функционалом IPS”

Gartner®

Источник:“Defining Next-Generation Network Intrusion Prevention,” Gartner, October 7, 2011.
“Defining the Next-Generation Firewall,” Gartner, October 12, 2009

Ответ предприятия › Антивирус (Host-Based) | IDS/IPS (Сетевой периметр) | Репутация (Global) и песочница | Разведка и аналитика (Облако)

Угрозы

Черви и вирусы

2000

Шпионское ПО и руткит

2005

APTs и кибервойны

2010

Изменение ландшафта угроз

завтра

ЭВОЛЮЦИЯ УГРОЗ