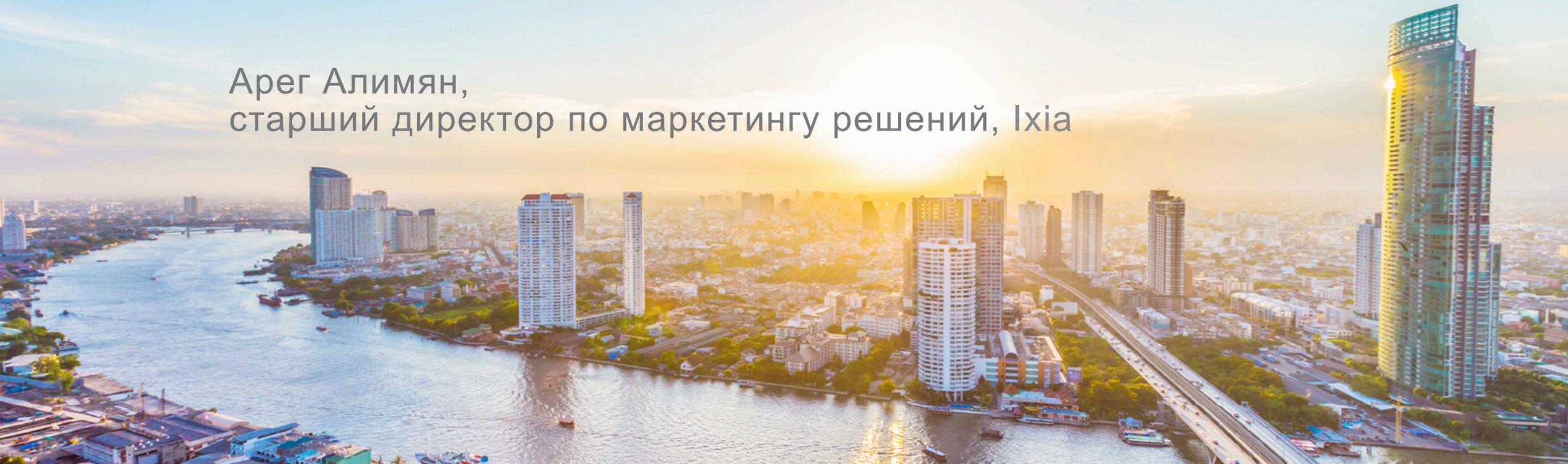




ПРЕДСТАВЛЕНИЕ КОМПАНИИ IXIA. ТЕНДЕНЦИИ SDN/NFV И РЕШЕНИЯ IXIA

Арег Алимян,
старший директор по маркетингу решений, Ixia



Достижения и глобальный масштаб компании Ixia

ВСЕГО
\$517
МИЛЛИОНОВ

ИСТОРИЯ

Год основания: 1997

Биржевое название: XXIA

Основные приобретения:

- Catapult Comm. (2009)
- VeriWave (2011)
- Anue Systems (2012)
- BreakingPoint (2012)
- Net Optics (2013)



6000+
КЛИЕНТОВ
ПО ВСЕМУ
МИРУ

1-ая
ПО
ИННОВАЦИЯМ
НА РЫНКЕ

#1
ЛИДЕР
РЫНКА

PROVE I.T. WITH IXIA

Самые именитые участники сетевого рынка доверяют продукции Ixia

15

из Top 15 NEMs

45

из Top 50 операторов

76

из Fortune 100

Корпоративные ИТ-системы/ЦОДы

Беспроводные и проводные сети

Наборы микросхем и устройства

ТЕНДЕНЦИИ РЫНКА

ОБЛАКА

БЕЗОПАСНОСТЬ
СЕТЕЙ

ВИРТУАЛИЗАЦИЯ

ИНТЕРНЕТ
ВЕЩЕЙ

90%

МОБИЛЬНОГО ТРАФИКА
ДАННЫХ БУДЕТ ОТНОСИТЬСЯ
К **ОБЛАЧНЫМ ПРИЛОЖЕНИЯМ**
В 2018 Г.

48%

РОСТ ЧИСЛА
ИНЦИДЕНТОВ
БЕЗОПАСНОСТИ
ПО ВСЕМУ МИРУ

80%

ПОКУПОК СОСТАВЯТ
СЕТИ SDx
В 2020 Г.

6

МИЛЛИАРДОВ
ПОДКЛЮЧЕННЫХ
ВЕЩЕЙ БУДУТ НУЖДАТЬСЯ
В ПОДДЕРЖКЕ В 2018 Г.

ШИРЕ РАСПРОСТРАНЕНИЕ = БОЛЬШЕ УЯЗВИМОСТЕЙ В СЕТИ

ПРОБЛЕМЫ ЗАКАЗЧИКОВ

Во что обходится плохо спроектированная, неконтролируемая и незащищенная сеть:

Возможность взлома Jeep заставила отозвать 1,4 млн машин и вызвала реакцию Конгресса.

Взлом системы OPM : раскрытие информации о 4 миллионах государственных служащих США.

Хакеры получили доступ к медицинским картам 1/3 американцев.

2,5 миллионов людей имеют имплантированные медицинские приборы с Wi-Fi. Все ли они протестированы?



СМОТРИТЕ ВНУТРЬ ЗАШИФРОВАННОГО ТРАФИКА

Пропустил угрозу – попал в новостную колонку

По оценкам Gartner, в 2017 году для обхода средств защиты более половины атак на корпоративные сети будут осуществляться с использованием зашифрованного трафика. Сегодня таких атак менее 5%.

SONY

Data compromised

Seemingly everything stored in the network.

How they got in – Unknown.

How long they went undetected – Unknown.

How they were discovered –

On Nov. 22 employee computers received messages threatening public distribution of stolen data and displays of skulls on their screens.

TARGET

Data compromised -

40 million credit and debit cards, 70 million phone numbers, mailing addresses and email addresses.

How they got in – Hacking the credentials of a legitimate business associate, an HVAC company, to get on Target's network, then installing malware on point-of-sale machines..

How long they went undetected – About two weeks.

How they were discovered –

How they were discovered – The Department of Justice told them about it, but anti-malware software flagged the problem as well.

THE HOME DEPOT

Data compromised - As many as

J.P.Morgan

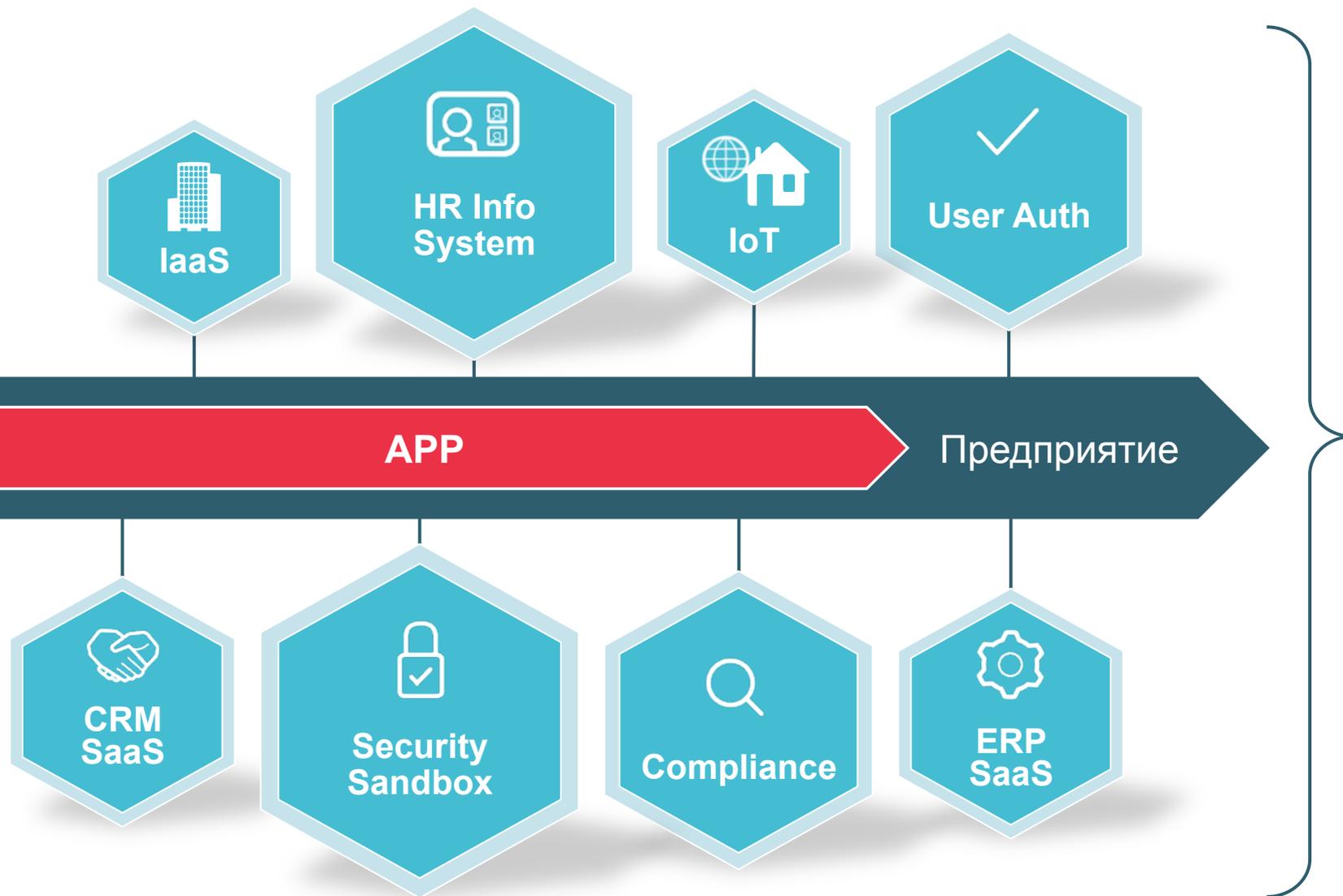
Data compromised - An



Ministry of Defence

They were blind to attacks coming inside encrypted traffic. Brought in Ixia to expand visibility. They took back control without having to buy a new security tool. Strengthened their security and saved money with Ixia

СОВРЕМЕННАЯ СРЕДА ПРИЛОЖЕНИЙ

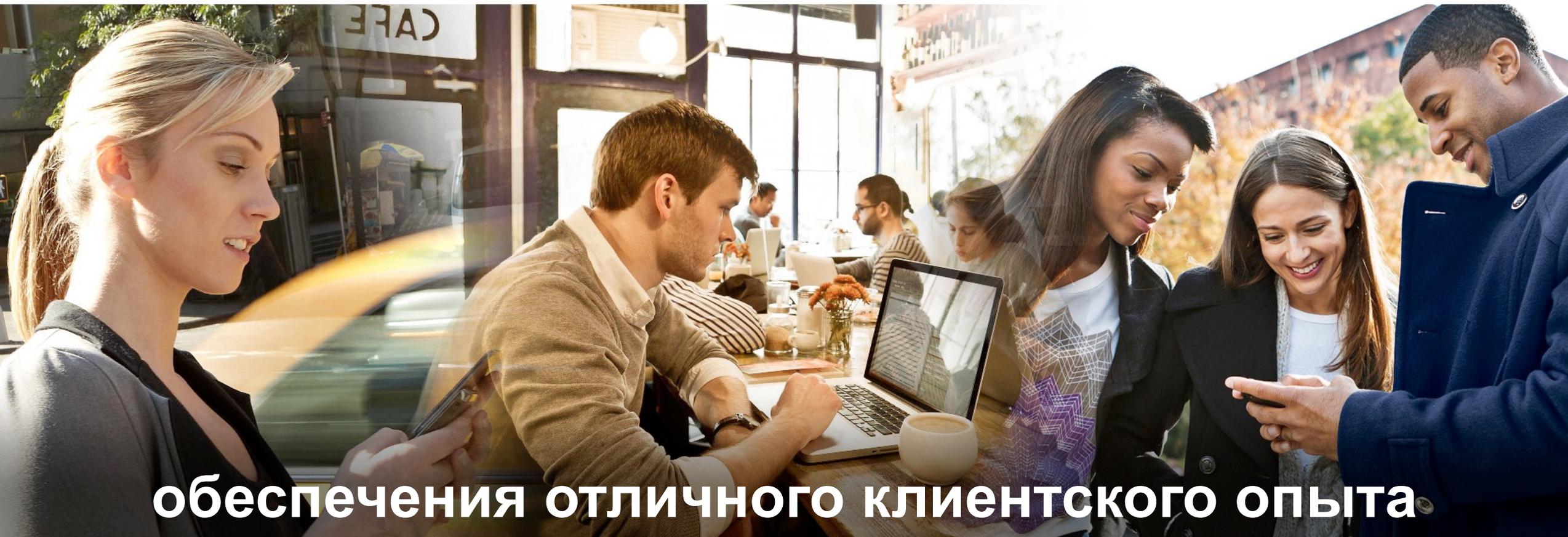


Больше устройств.

Больше данных.

**Больше надо
защищать.**

УСПЕХ ВАШЕГО БИЗНЕСА ЗАВИСИТ ОТ



обеспечения отличного клиентского опыта

НАДЕЖНОСТЬ БЫСТРОТА БЕЗОПАСНОСТЬ

WE MAKE APPLICATIONS STRONGER

Лучшая основа позволяет снизить совокупную стоимость владения

ТЕСТИРОВАНИЕ



\$2,5 М

Экономия OPEX в связи с использованием средств ИБ – TCO за три года.

ЗАЩИТА



\$300 К

Ежегодная экономия OPEX и 15-кратное увеличение ROI за счет использования ThreatARMOR в качестве первой линии защиты.

МОНИТОРИНГ



\$800 К

3-годичная экономия OPEX за счет установки инфраструктуры мониторинга и 10X рост ROI.

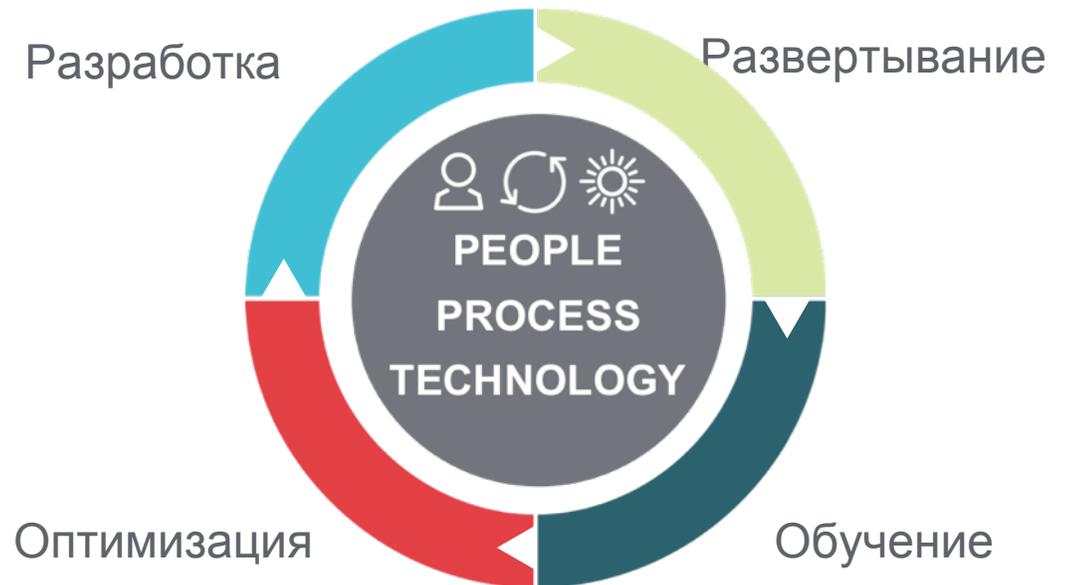
КАК ОБЕСПЕЧИТЬ НАДЕЖНОСТЬ, БЫСТРОТУ И БЕЗОПАСНОСТЬ СЕРВИСОВ? ПОСРЕДСТВОМ 360° ТЕСТИРОВАНИЯ

Сквозное (end-to-end) тестирование



Тестирование всей экосистемы или отдельных устройств

Непрерывное тестирование



Тестирование в течение всего жизненного цикла

360-градусное тестирование – чтобы доверять своим решениям!

СНИЖЕНИЕ ЗАТРАТ ЗА СЧЕТ РАННЕГО ОБНАРУЖЕНИЯ ДЕФЕКТОВ

90x ROI

ПРИ РАННЕМ ОБНАРУЖЕНИИ ДЕФЕКТОВ

РАННЕЕ ОБНАРУЖЕНИЕ ЭКОНОМИТ ДЕНЬГИ



КЛИЕНТСКИЙ СЛУЧАЙ

Проверка защиты от DDoS-атак. Финансовая биржа

Клиент

- Крупная площадка для торговли деривативами.
- Контракты на 3 млрд долларов ежегодно.

Потребность

- Проверка поставщика услуг по защите от DDoS-атак.
- Сокращение времени подавления атак.
- Повышение готовности к отражению кибератак.

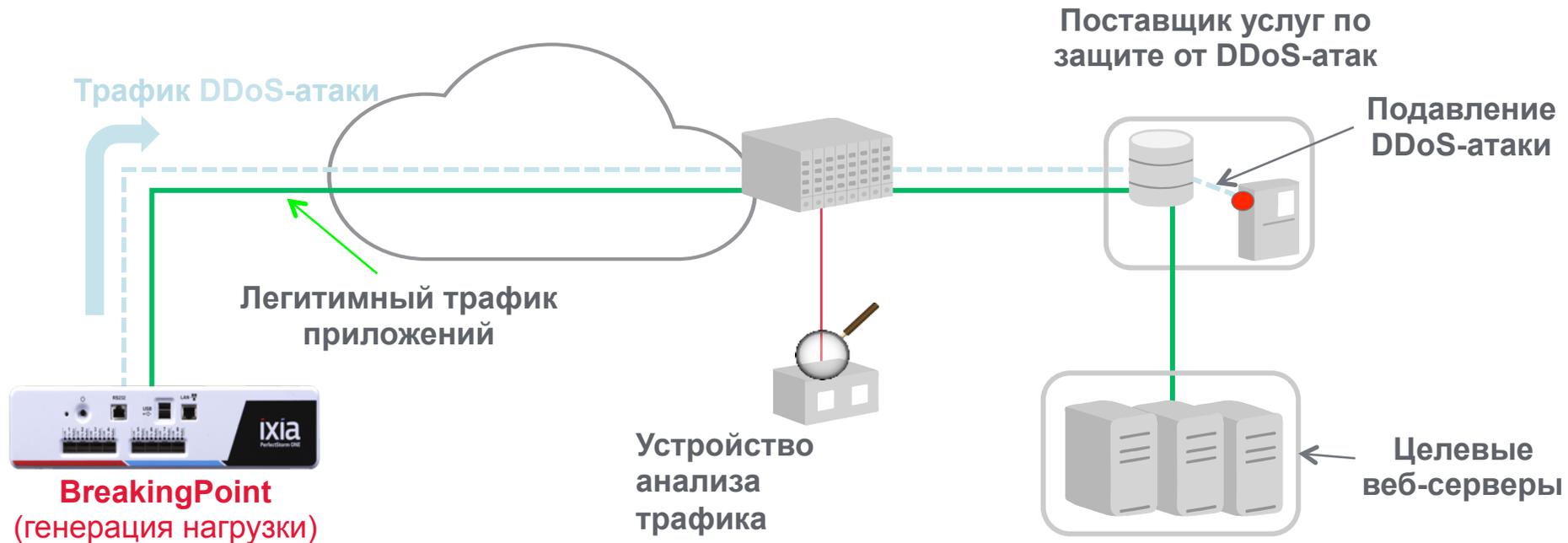
Результат

- **10-кратное повышение** скорости активации защиты от DDoS-атак.
- Повышенная устойчивость к кибератакам.



КЛИЕНТСКИЙ СЛУЧАЙ

Проверка защиты от DDoS-атак. Финансовая биржа



КЛИЕНТСКИЙ СЛУЧАЙ

Проверка защиты от DDoS-атак. Финансовая биржа

“Продукт Ixia BreakingPoint предотвратил большой сбой в обслуживании и помог нам значительно повысить эффективность нашего сервиса анти-DDoS”



КЛИЕНТСКИЙ СЛУЧАЙ

Оценка продукта. Многонациональная корпорация

Клиент

- 100 тыс. сотрудников.
- Сферы деятельности: энергетика, потребительские товары и финансы.

Потребность

- Максимальное повышение надежности обновлений сети.
- Гарантия от неприятных сюрпризов.

Результаты

- Клиент смог избежать установки нового микропрограммного обеспечения, которое привело бы к снижению производительности на 80%.
- Клиент получил информацию для взаимодействия с производителем для решения проблемы.

ПРИНИМАЙТЕ РЕШЕНИЯ НА ОСНОВЕ ФАКТОВ

10X различие в затратах – TCO на каждый защищенный Мбит/с – от 50 до 541 долл.
NSS Labs Breach Detection Systems Comparative Report, Aug 2015

\$2,5 M+
ЭКОНОМИЯ TCO через 36 месяцев

Изменение эффективности защиты от 99,2 до 51,8% повышает риск раскрытия данных.
Ponemon Institute, 2015

\$7,2 M
СРЕДНИЙ УБЫТОК ОТ УТЕЧКИ ДАННЫХ

Оптимизируйте процессы, минимизируйте простои для сокращения MTTR.
Ponemon Institute, 2015

\$300 K+
УБЫТОК ОТ ЧАСОВОГО ПРОСТОЯ

**УСТРАНЯЙТЕ НЕИЗВЕСТНОЕ,
МИНИМИЗИРУЙТЕ РИСК И МАКСИМИЗИРУЙТЕ
ЭКОНОМИЮ**

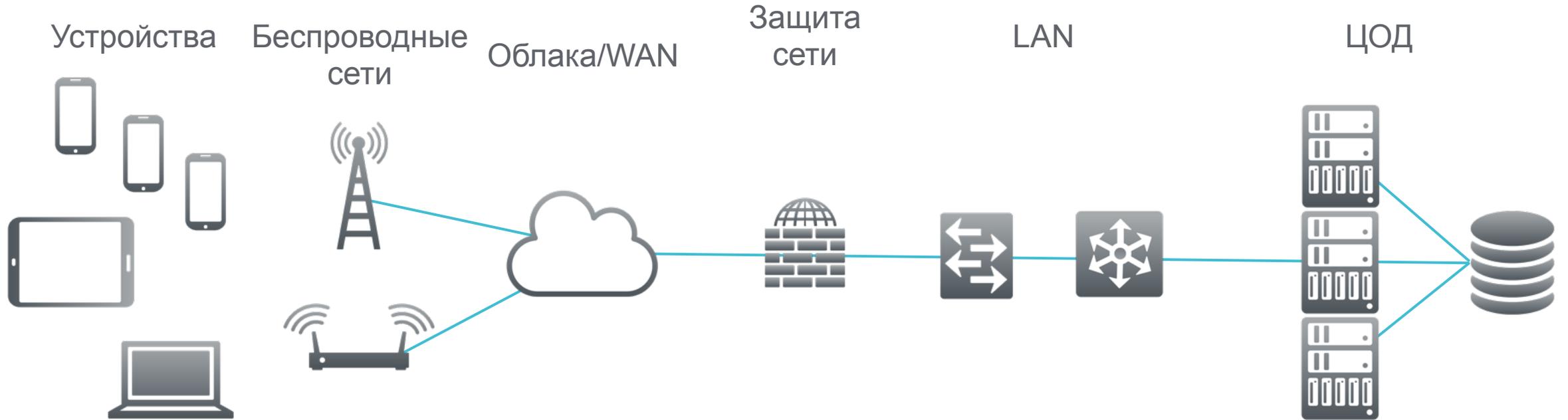
ROI: 40x

IXTEST: ПРОВЕРЯЙТЕ С ПОМОЩЬЮ 360° ТЕСТИРОВАНИЯ



Исследовательский центр АТІ

РЕШЕНИЯ IXIA ДЛЯ 360° ТЕСТИРОВАНИЯ



Производительность и надежность сети Wi-Fi



IxVeriWave

Производительность инфраструктуры



IxLoad/IxChariot

Эмуляция WAN



Network Emulator II

Устойчивость к атакам



BreakingPoint

Переход на SDN/NFV



IxNetwork

QoE при работе с приложениями, масштабируемость и производительность ЦОДа



IxLoad & IxNetwork

ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР APPLICATION & THREAT INTELLIGENCE

300+ семейств сигнатур приложений.

Идентификация приложений
в реальном времени.

Изоляция неизвестных приложений.

ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР
APPLICATION AND
THREAT INTELLIGENCE

Богатые метаданные
о контекстном поведении.
Эмуляция сотен приложений
для мониторинга.

Досье на плохие IP-адреса.

I ИНТЕЛЛЕКТ IXIA

- Инженеры Ixia.
- Производители средств ИБ.
- Потoki от пакетных брокеров.
- Взаимодействие с NEMs.

ИССЛЕДОВАТЕЛЬСКИЕ ЛАБОРАТОРИИ ПО БЕЗОПАСНОСТИ

ГЛОБАЛЬНАЯ СЕТЬ HONEYROT'ОВ И ПОИСКОВЫХ РОБОТОВ

ИСТОЧНИКИ БОЛЬШИХ ДАНЫХ

- Миллиарды IP-адресов и URL.
- Миллионы SPAM.
- Наборы данных из открытых источников.
- Вторжения в сети.

Периодическое обновление | **Новые** приложения | **Новые** плохие IP-адреса

МОНИТОРИНГ (VISIBILITY)

“Идентификация проблем – самая трудная задача для ИТ-специалистов”

Зевс Керравала,
главный аналитик, ZK Research

“Время, затрачиваемое на идентификацию проблемы, составляет 85% MTTR”

ТИПИЧНАЯ СИТУАЦИЯ С МОНИТОРИНГОМ



Участвующие группы

Network
Ops

Application
Ops

Администраторы
безопасности

Администра-
торы серверов

Forensics

Privacy &
Audit



Множество используемых средств

NPMD

APM

Customer
Experience

Forensics

IDS,
SIEM

Firewall,
IPS



Среда, которой всё сложнее управлять

Оконечные
узлы



Сеть



ЦОД



Облако

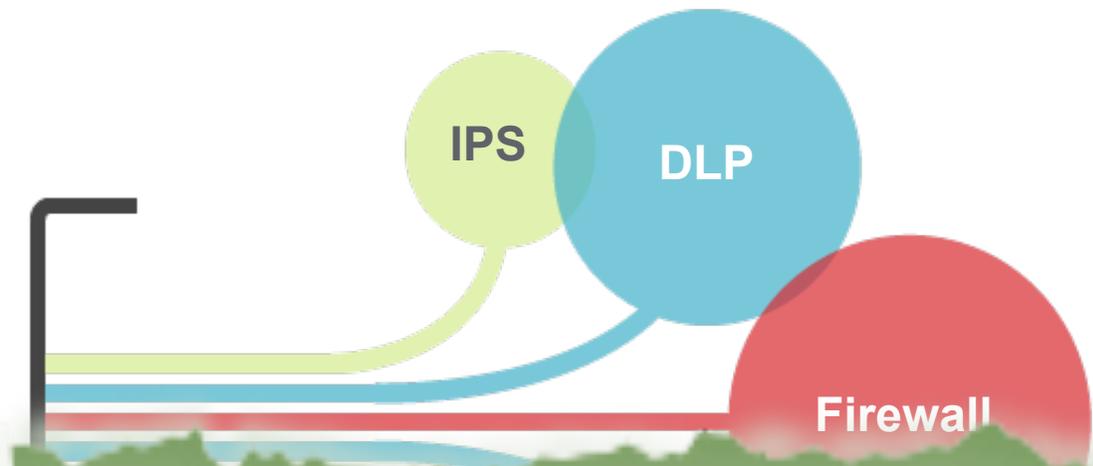
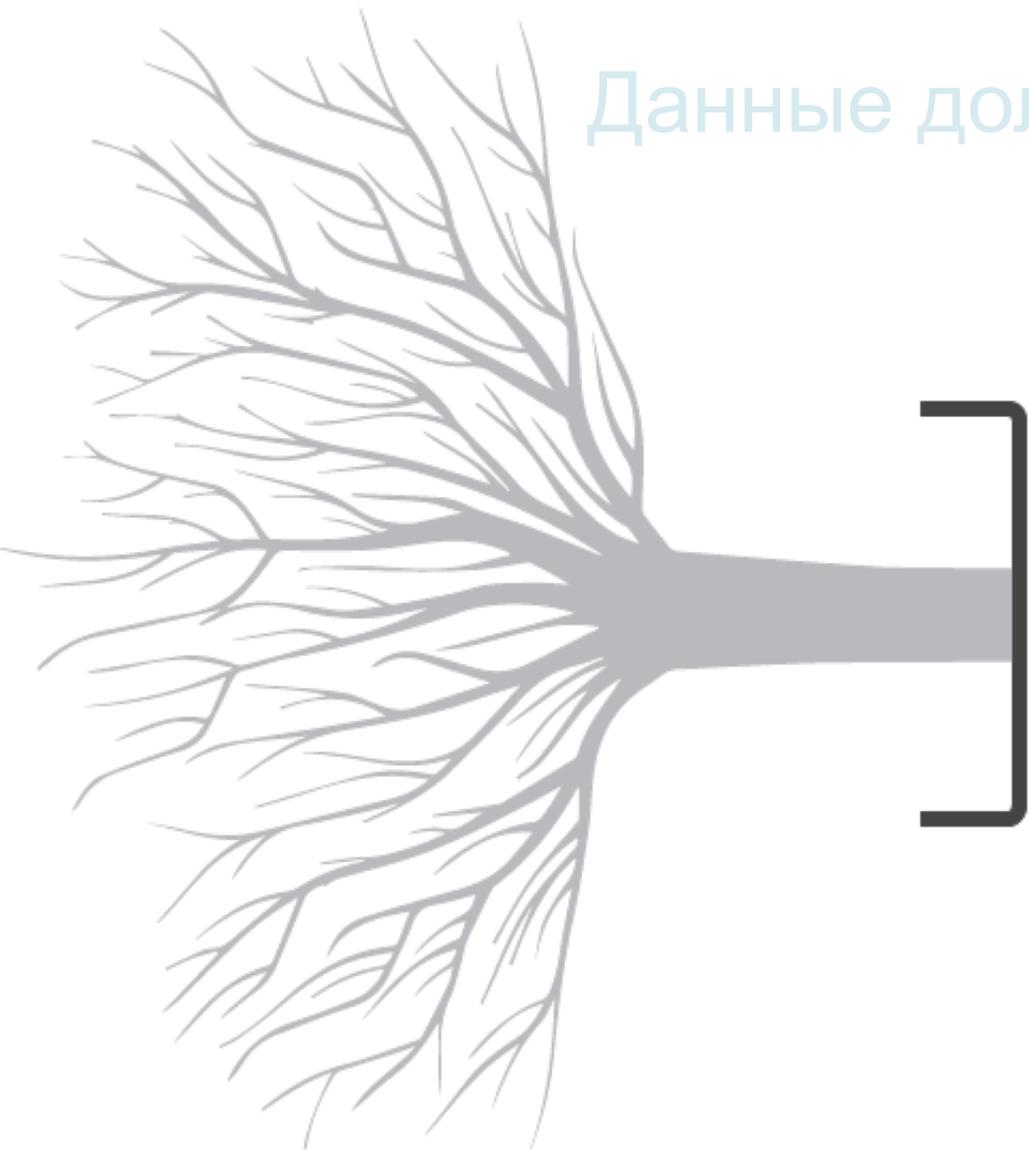


Приложения



ПОТРЕБНОСТЬ ВИДЕТЬ ВСЁ

Данные должны попасть на устройства ИБ



Allstate

You're in good hands.

Put in a new security deployment. Tool costs were prohibitive. Brought in Ixia to 'extend the reach' of the tools. Achieved it in 1/2 the cost. With fewer tools. And without sacrifice

#securitywithout sacrifice

ТИПИЧНЫЕ РЕЗУЛЬТАТЫ МОНИТОРИНГА

79%

НЕ получают
оптимальный результатов
от инвестиций в АРМ¹

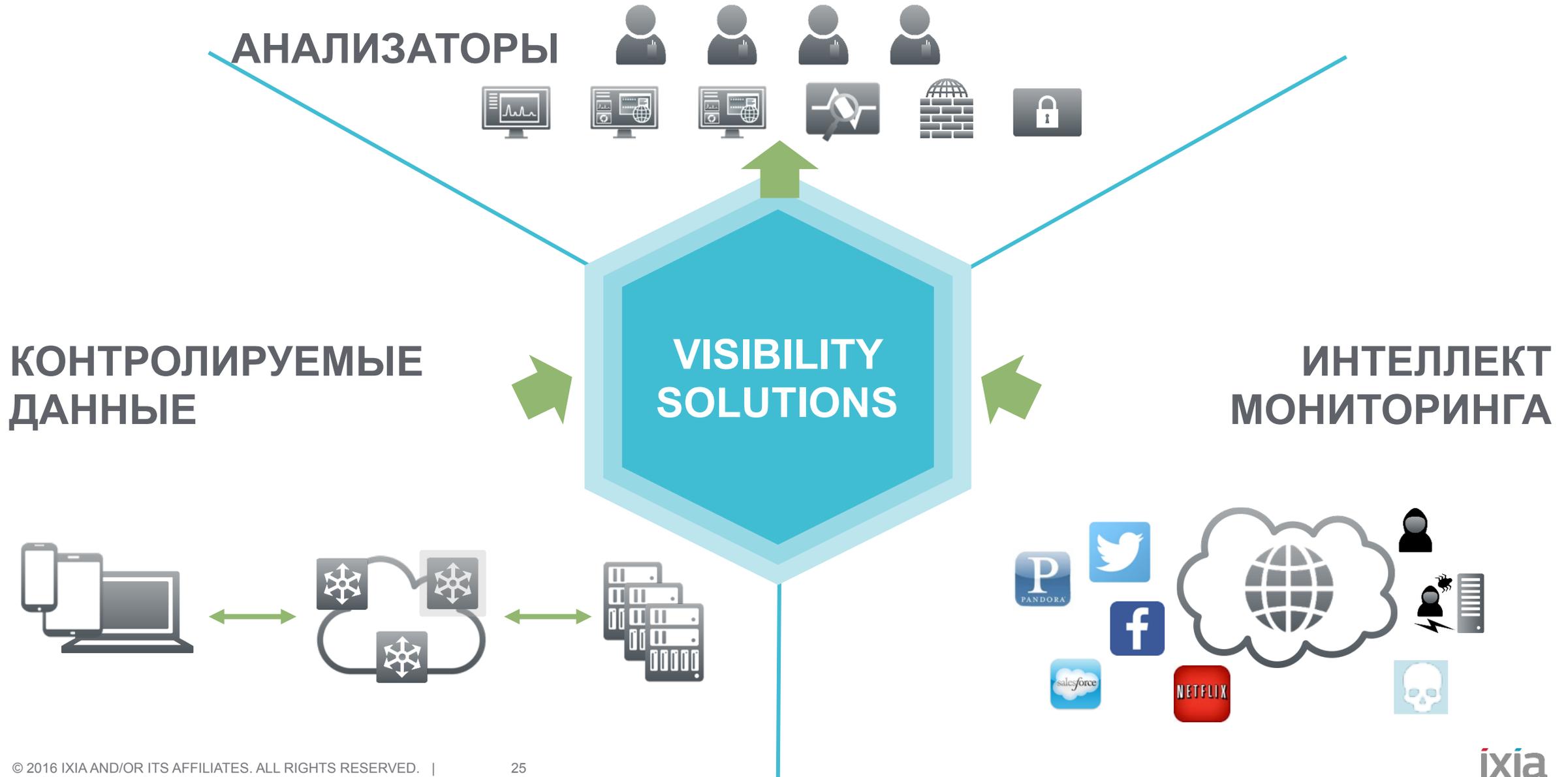
Сложность

Неэффективность

Затратность

Сохранение
«слепых пятен»

МОДЕЛЬ ДЛЯ УЛУЧШЕНИЯ МОНИТОРИНГА



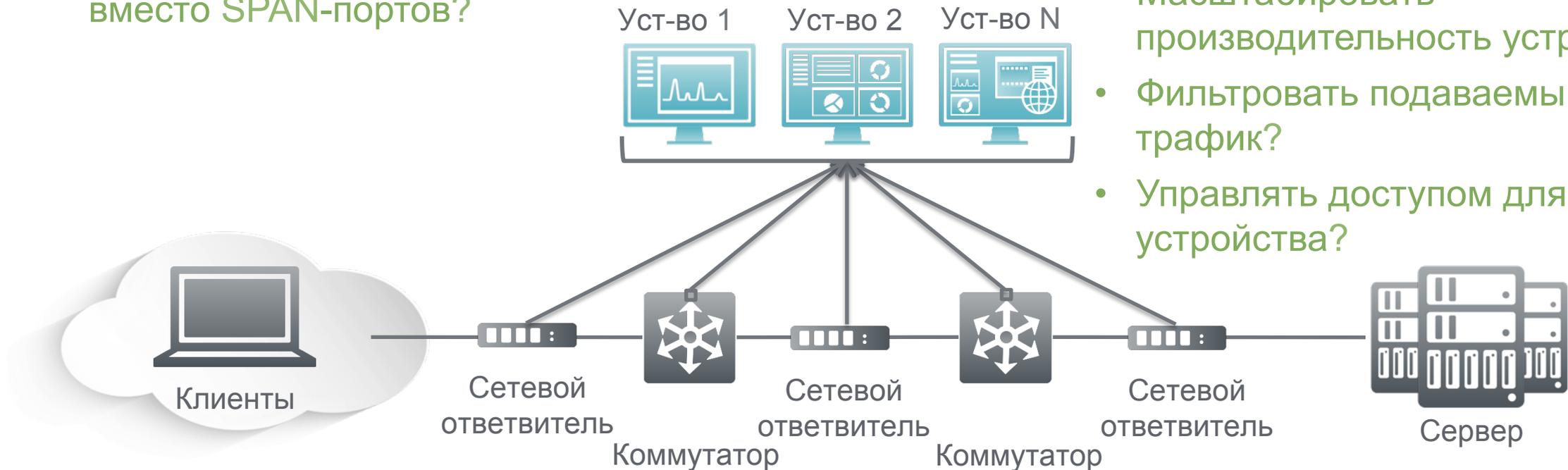
ИНТЕЛЛЕКТУАЛЬНЫЙ МОНИТОРИНГ

Как:

- Обеспечить доступ к данным для устройств мониторинга?
- Использовать ответвители вместо SPAN-портов?

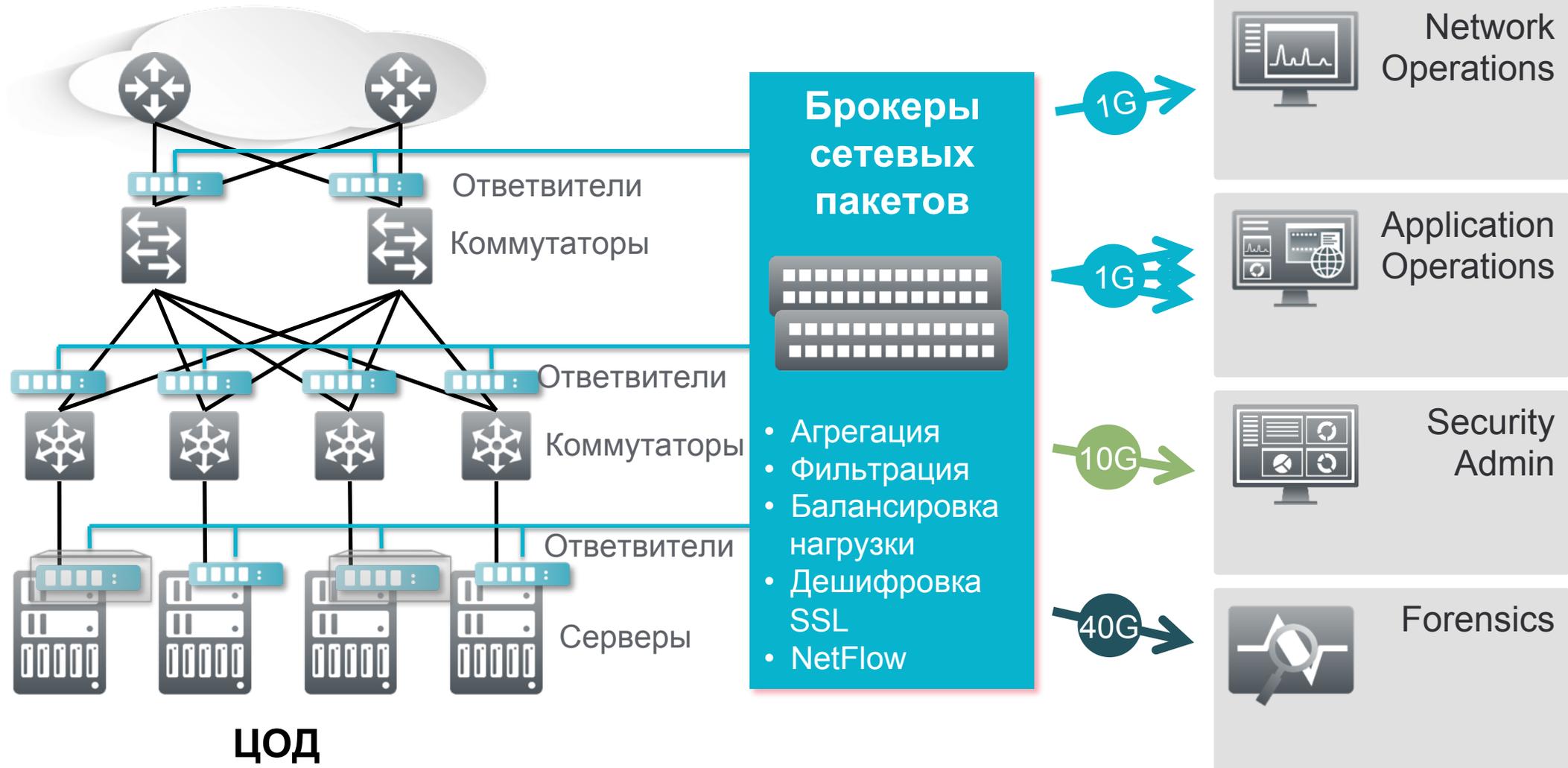
Как:

- Выходить из положения при ограниченном числе портов в устройствах?
- Масштабировать производительность устройств?
- Фильтровать подаваемый на них трафик?
- Управлять доступом для каждого устройства?



ИНТЕЛЛЕКТУАЛЬНЫЙ МОНИТОРИНГ

Доступ к данным по всей сети, распределение данных



КЛИЕНТСКИЙ СЛУЧАЙ

Техасский университет в Остине

Клиент

- 5-й по величине кампус в США – более 50 тыс. студентов.
- Более 24 тыс. сотрудников.

Потребность

- Мониторинг больших объемов трафика приложений.
- Контроль расходов на анализ трафика.
- Повышение общей эффективности Incident Response Team.

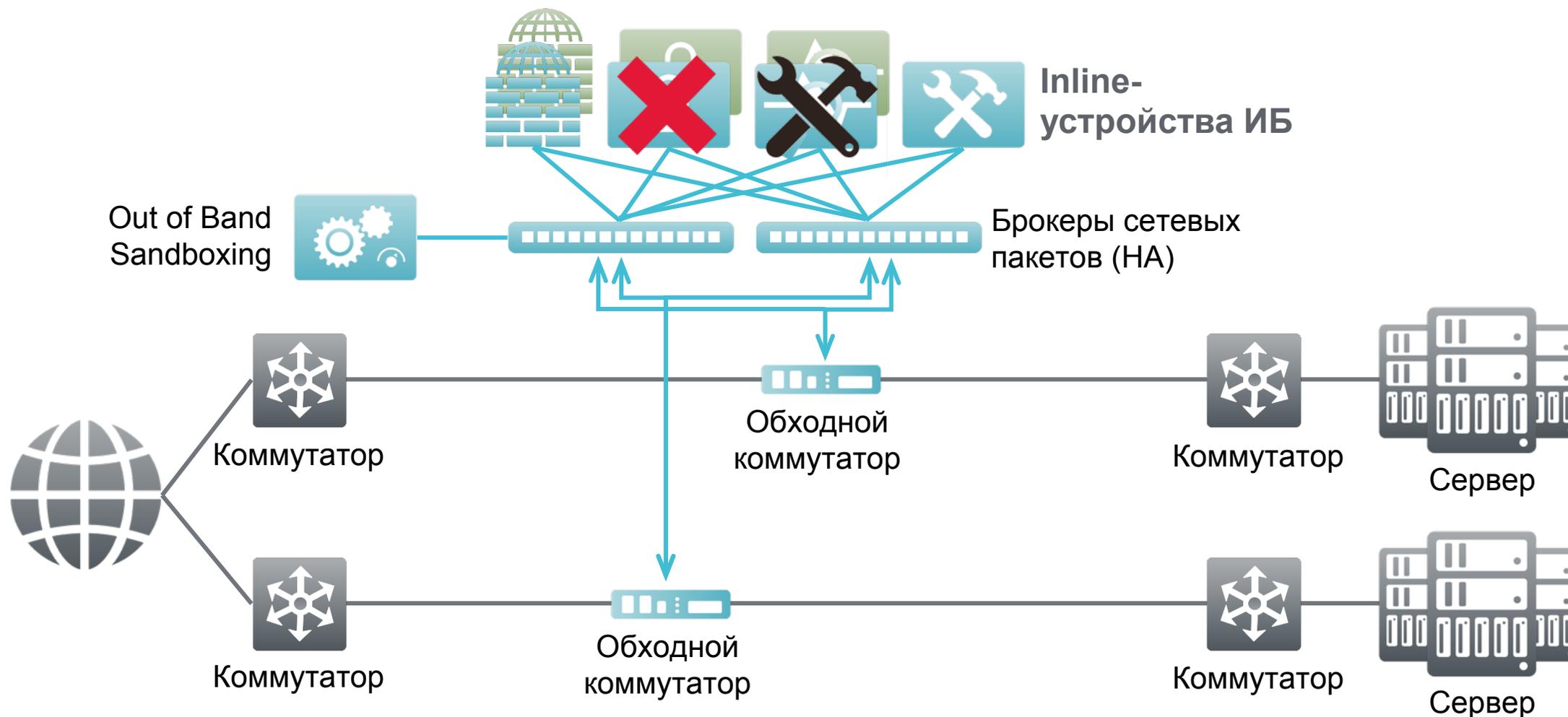
Результат

- Развернуты интеллектуальные решения Ixia, включая NTO 7300 и ATIP.
- Потребовалось на 20–30% меньше емкости систем IDS.
- Уменьшены плановые капитальные затраты на системы IDS.
- Проект полностью окупился.



ЭЛАСТИЧНАЯ СИСТЕМА ИБ

Схема эластичной системы ИБ



КЛИЕНТСКИЙ СЛУЧАЙ

Компания по технологиям и решениям для обработки платежей

Клиент

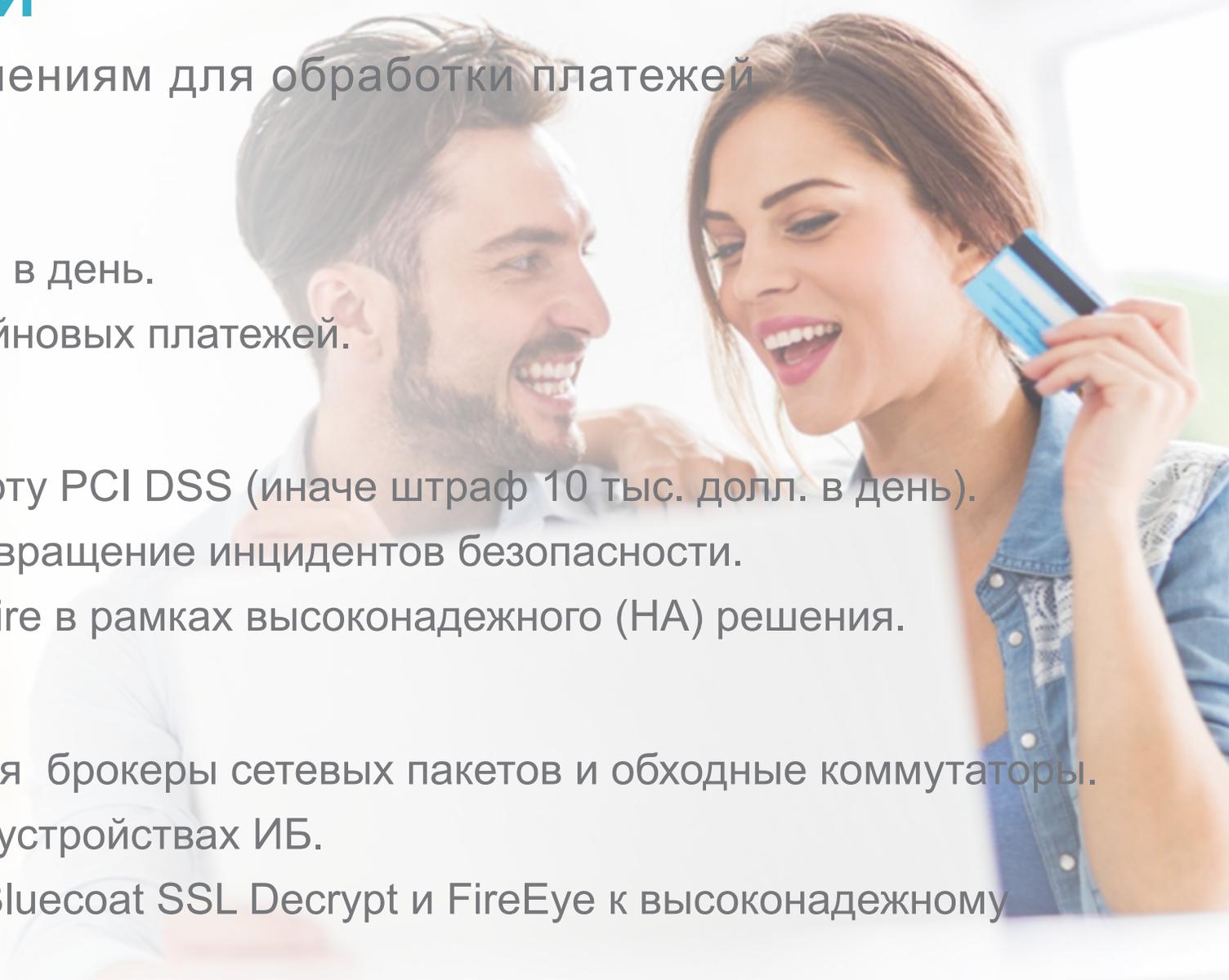
- Сеть выполняет 30 млн транзакций в день.
- Лидер в области карточных и онлайн-платежей.

Потребность

- Обеспечение соответствия стандарту PCI DSS (иначе штраф 10 тыс. долл. в день).
- Улучшение контроля сети и предотвращение инцидентов безопасности.
- Развертывание IPS-систем Sourcefire в рамках высоконадежного (HA) решения.

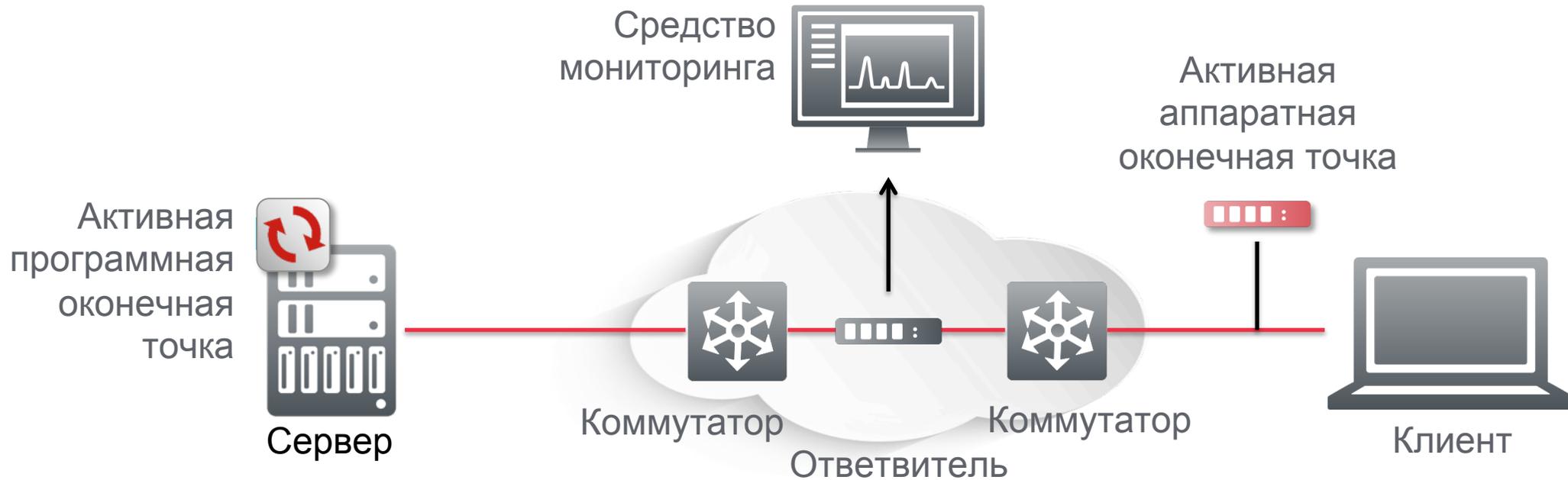
Результаты

- Установлены продукты Ixia, включая брокеры сетевых пакетов и обходные коммутаторы.
- Сэкономлено 3 млн долл. на inline-устройствах ИБ.
- Добавлены защитные устройства Bluescoat SSL Decrypt и FireEye к высоконадежному решению.
- Проект 10-кратно окупился.



ПРОАКТИВНЫЙ МОНИТОРИНГ

Возможность контроля при отсутствии контролируемого сетевого трафика.



- Генерация трафика сотен типов приложений.
- Возможность задавать требования SLA и контролировать их выполнение.
- Только Ixia предлагает такие решения.
- Простота и экономическая эффективность.

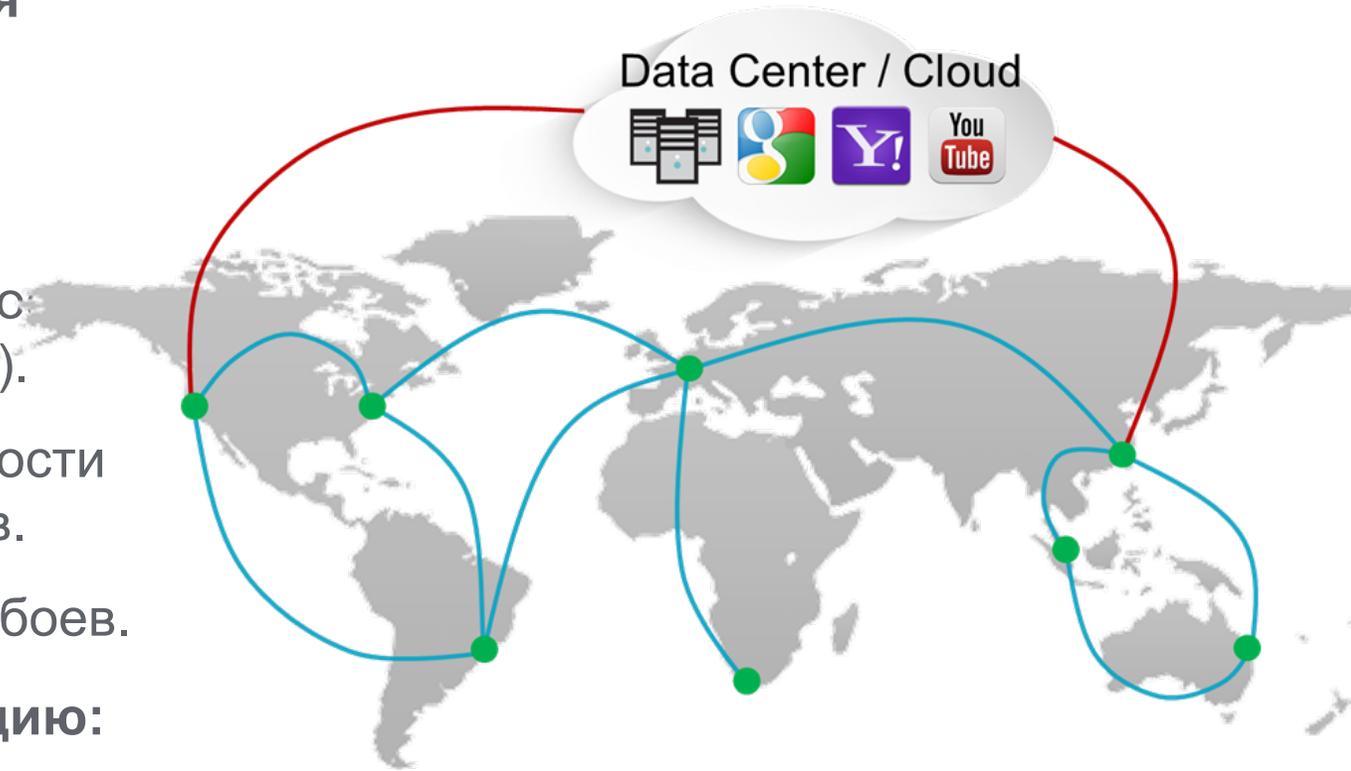
ПРОАКТИВНЫЙ МОНИТОРИНГ

Постоянная полезность для выполнения сетевых операций:

- Мониторинг SLA и клиентского опыта в глобальном масштабе.
- Контроль надежности и производительности соединений между узлами (площадками).
- Контроль надежности и производительности приложений, ЦОДов, облачных сервисов.
- Проактивное обнаружение и изоляция сбоев.

Уверенность перед вводом в эксплуатацию:

- Определение базовых характеристик сети и сервисов.
- Оценка готовности сети к внедрению новых сервисов.
- Проверка сервиса (например, Skype, ISP) перед его запуском.



— Приложение/ЦОД/облако
— Узел – узел

КЛИЕНТСКИЙ СЛУЧАЙ

Крупная компания, занимающаяся управлением активами и страхованием

Клиент

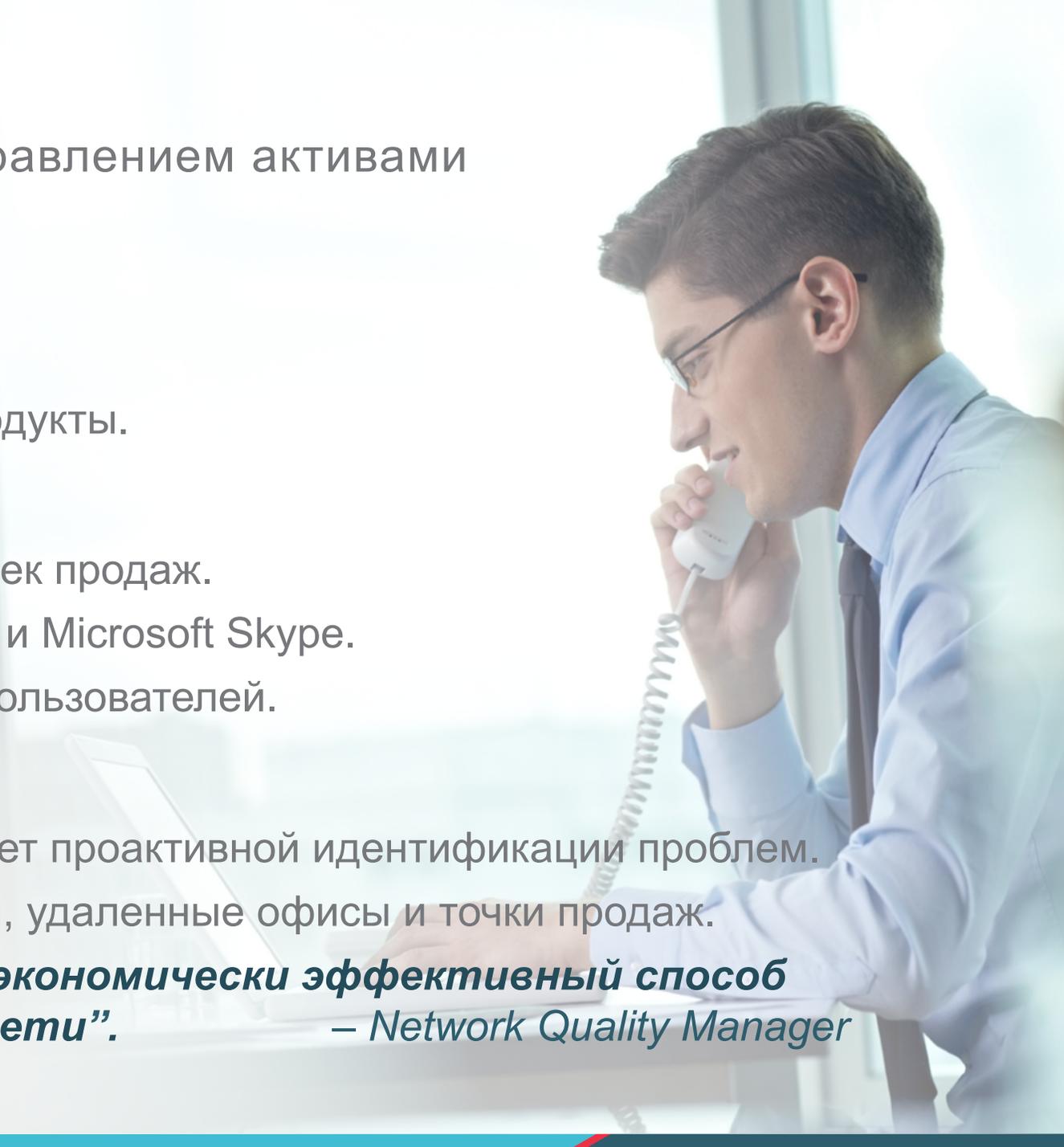
- Обслуживает клиентов более 158 лет.
- Продает страховые и инвестиционные продукты.

Потребность

- Поддержка сотен удаленных офисов и точек продаж.
- Глобальное использование сервисов VoIP и Microsoft Skype.
- Гарантия соответствия услуг ожиданиям пользователей.

Результат

- 99% соответствие требованиям SLA за счет проактивной идентификации проблем.
- Глобальный мониторинг SLA – HQ, шлюзы, удаленные офисы и точки продаж.
- ***“Использование решения Ixia – самый экономически эффективный способ мониторинга нашей распределенной сети”.*** – Network Quality Manager



Простота конфигурирования

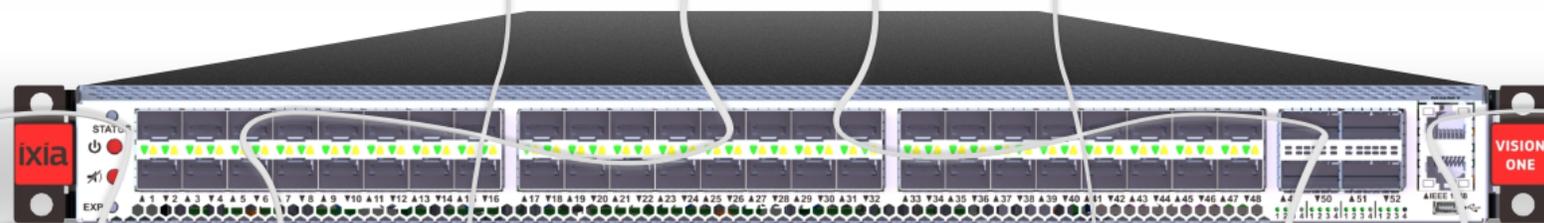
Интуитивный UI и
запатентованный
компилятор
фильтров

Полный контроль трафика

API для
расшифровки SSL и
интеллектуальной
работы на уровне
приложений

Постепенное наращивание

Балансировка
нагрузки в
пределах групп
устройств и
между ними



Гибкое подключение
inline- и out-of-band-
устройств

Многоуровневая
защита

VisionONE™

Обработка
пакетов без их
потерь и DPI

Фокус на то, что важно

The logo for ixia, featuring the lowercase letters 'ixia' in a white, sans-serif font. The 'i' has a red dot, and the 'x' has a blue dot. The logo is positioned on the left side of the image, partially overlapping a 3D blue cube.

ixia

ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР АТИ

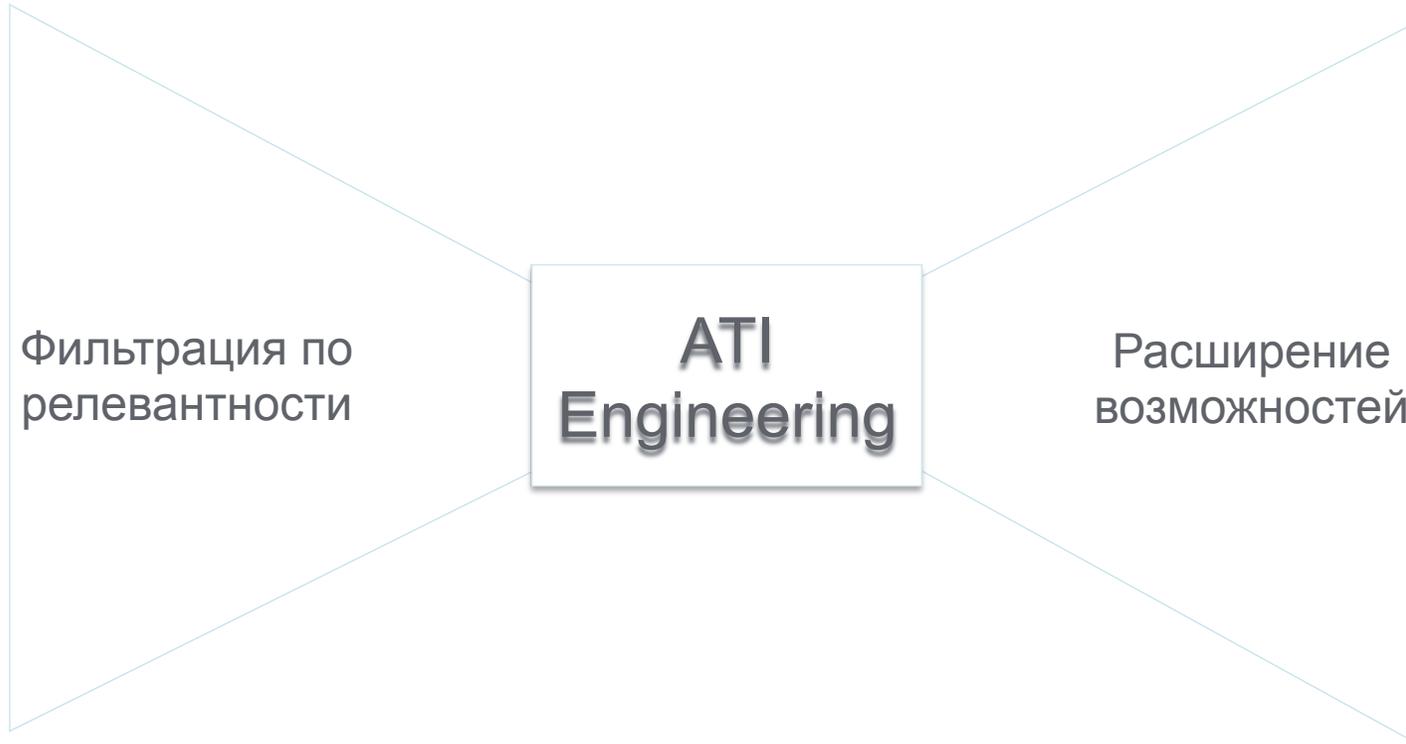
ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР АТИ



ATI I/O

Вход

Новости
Клиенты
Отчеты
Активность
в Интернете



Выход

Продукты
Обучение
Отчеты
Практическая
информация

IMPORTANT JUNIPER SECURITY ANNOUNCEMENT

CUSTOMER UPDATE: DECEMBER 20, 2015

Administrative Access (CVE-2015-7755) only affects ScreenOS 6.3.0r17 through 6.3.0r20. VPN Decryption (CVE-2015-7756) only affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20.

We strongly recommend that all customers update their systems and apply these patched releases with the highest priority.

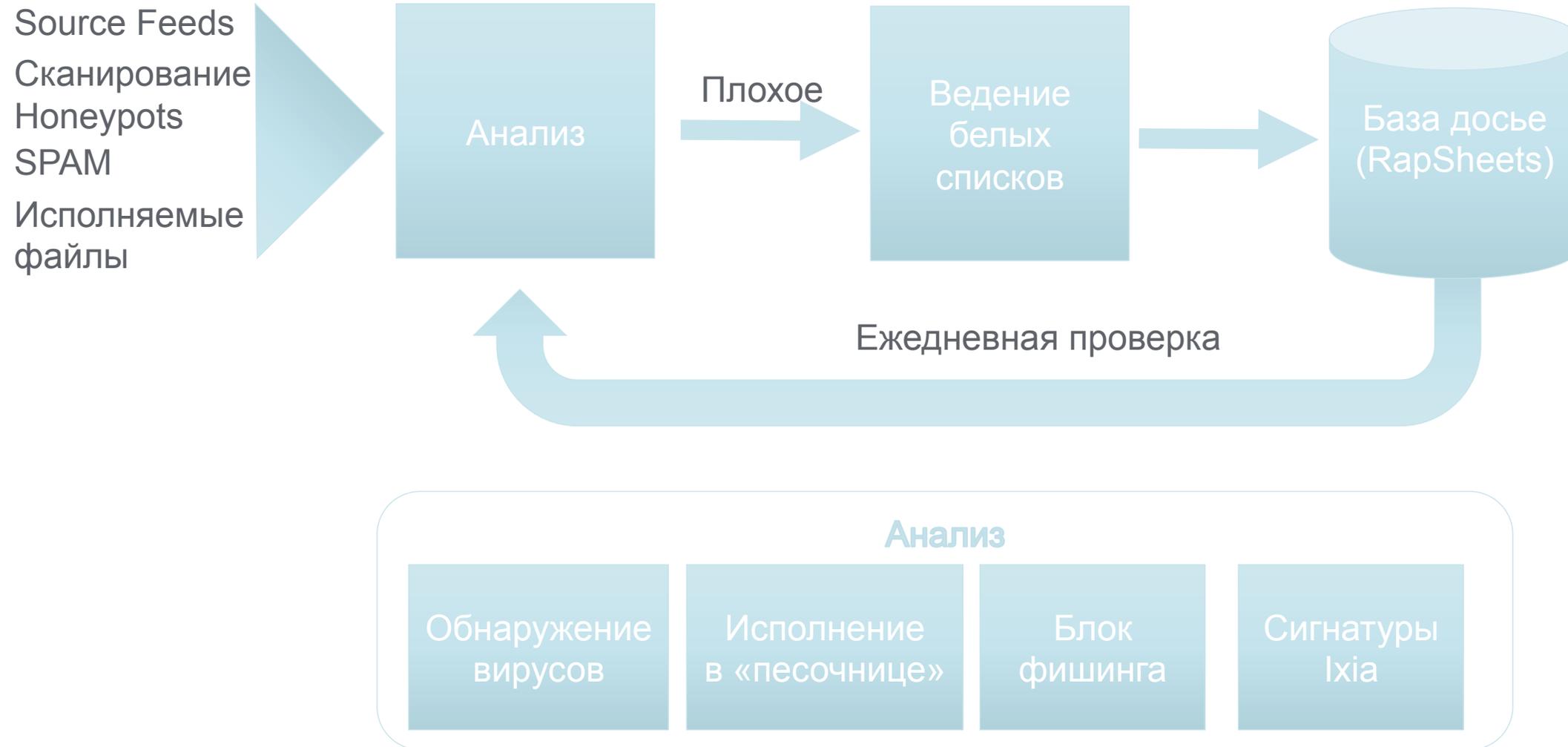
POSTED BY BOB WORRALL, SVP CHIEF INFORMATION OFFICER ON DECEMBER 17, 2015



18 декабря атака стала доступна

THREAT INTELLIGENCE

- ATI RapSheets идентифицируют и доказывают криминальные действия в Интернете



ЧТО ТАКОЕ APPLICATION AND THREAT INTELLIGENCE?

- Авангард Ixia, чтобы идти в ногу с Интернетом

- **Application**

- Протоколы.
- Смеси трафика приложений.



BreakingPoint Sandvine 1H 2013 Asia Pacific Fixed
BreakingPoint Sandvine 1H 2013 Asia Pacific Mobile
BreakingPoint Sandvine 1H 2013 Europe Fixed
BreakingPoint Sandvine 1H 2013 Europe Mobile
BreakingPoint Sandvine 1H 2013 Latin America Fixed
BreakingPoint Sandvine 1H 2013 Latin America Mobile
BreakingPoint Sandvine 1H 2013 NA Fixed
BreakingPoint Sandvine 1H 2013 NA Mobile
BreakingPoint Sandvine 1H 2014 Africa Fixed
BreakingPoint S
ngPoint S
ngPoint S

- **Threat**

- Атаки.



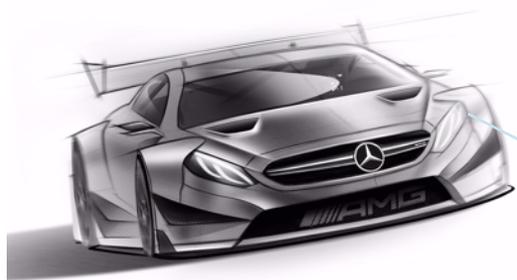
- **Intelligence**

- Вредоносные сайты.
- Методики защиты.



ATI 2015

БЫСТРЫЕ ВЫПУСКИ



- 26 обновлений ATI каждые 2 недели.
 - 49 новых приложений, 430 новых потоков, 689 новых атак.
- 12 ежемесячных Evergreen Updates.

- 12 ежемесячных обновлений AppLibrary.
 - 1347 потоков трафика приложений.

- 12 ежемесячных обновлений информации о вредоносных программах.

- 600 вредоносных программ.

- 8 выпусков информации о ботнетах.
 - 400 ботнетов.

- 281 ATIP-приложений.

Всего:

36 892 атак,
316 приложений,
3494 потоков.

Предоставляются для большинства продуктов Ixia:

1. NTS (тестовые решения)

- BPS
- IxLoad/IxNetwork AppLibrary
- IxLoad Attack PVM
- IxChariot/Hawkeye

2. NVS (решения для мониторинга)

- ATIP

3. Security (средства защиты сети)

- ThreatArmor





Threat**ARMOR**

ОБЕСПЕЧЕНИЕ ИБ

Классификация трафика Интернета

**В КАЖДУЮ СЕТЬ
ПОСТУПАЕТ ТРАФИК
ДВУХ ТИПОВ**

**ДОСТОЙНЫЙ
АНАЛИЗА ТРАФИК:**

потенциально интересный
трафик

**ТРАФИК, КОТОРЫЙ НЕ
СТОИТ АНАЛИЗИРОВАТЬ:**

**ОТ ИЗВЕСТНЫХ САЙТОВ,
РАСПРОСТРАНЯЮЩИХ
ВРЕДНОСНОЕ ПО**

С УКРАДЕННЫХ IP-АДРЕСОВ

С НЕВЫДЕЛЕННЫХ IP-АДРЕСОВ

ИЗ НЕЖЕЛАТЕЛЬНЫХ РЕГИОНОВ



Вложения в инфраструктуру безопасности растут в связи с ростом требований к ней



ИННОВАЦИИ В БЕЗОПАСНОСТИ СЛЕДУЮТ ЗА РАЗВИТИЕМ АТАК

Больше функций защиты. Больше сложность. Больше операций обслуживания. Больше задач управления.

НО, ЧТО ЕСЛИ УДАСТСЯ «СЖАТЬ» ИНТЕРНЕТ?

МЕНЬШЕ
АТАКУЮЩИХ

МЕНЬШЕ
ОПОВЕЩЕНИЙ ОТ
SIEM

МЕНЬШЕ
ПОВЕРХНОСТЬ
АТАКИ

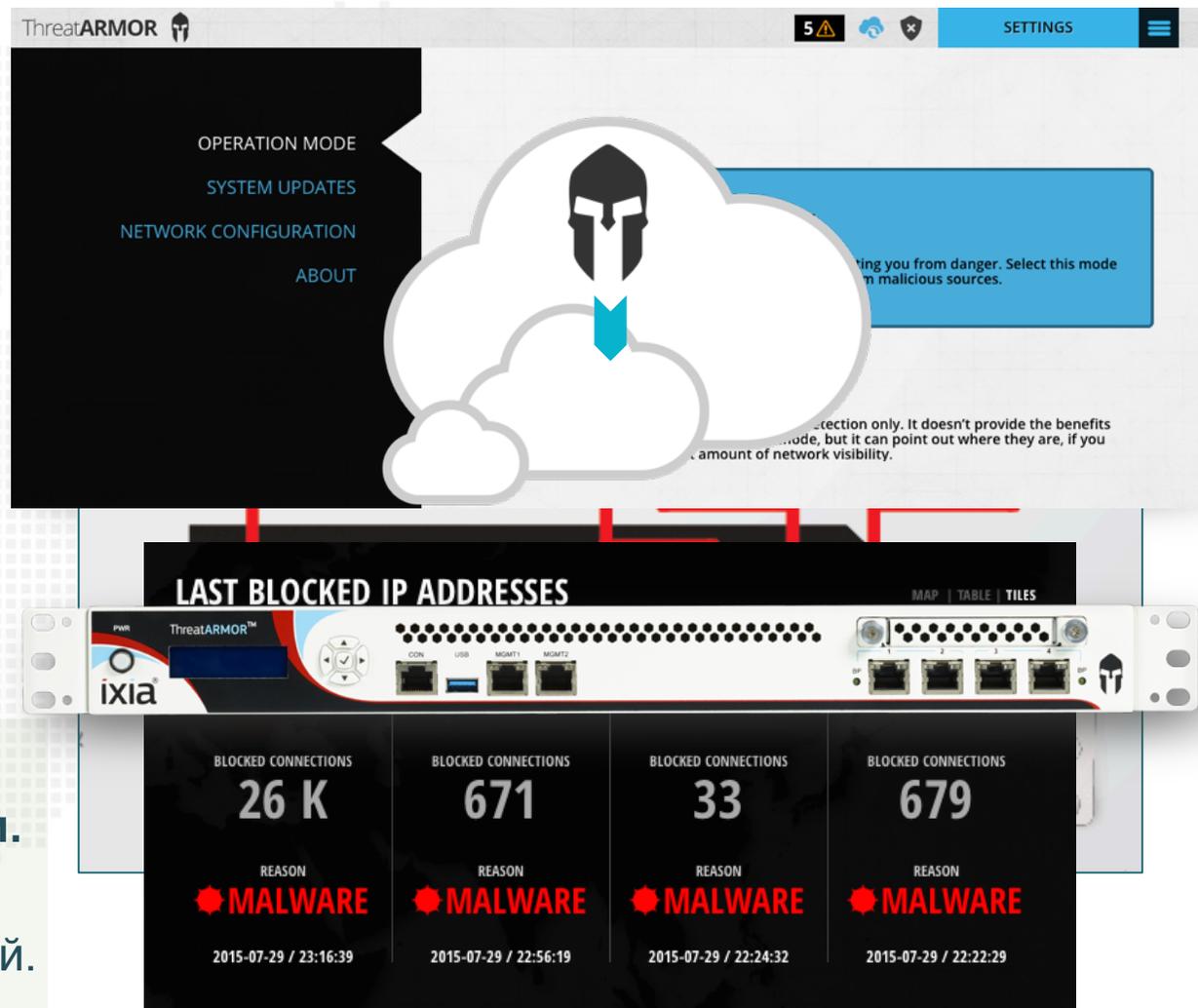
ИНФРАСТРУКТУРА БЕЗОПАСНОСТИ
может сфокусироваться на том, что важно

ПРОСТОТА УСТАНОВКИ

1. Подключите устройство к электророзеткам и кабелям Ethernet.
2. Выберите режим **Report Only Mode** или **Blocking Mode**.
3. На этом всё. Устройство автоматически загрузит информацию об угрозах ИБ.

Криминальные сайты блокируются **автоматически**.

Географическая блокировка является опциональной.



ЗОЛОТАЯ НАГРАДА В КОНКУРСЕ 2016 GLOBAL EXCELLENCE AWARDS® В ОБЛАСТИ ПРОДУКТОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ТЕНДЕНЦИИ SDN/NFV И РЕШЕНИЯ IXIA

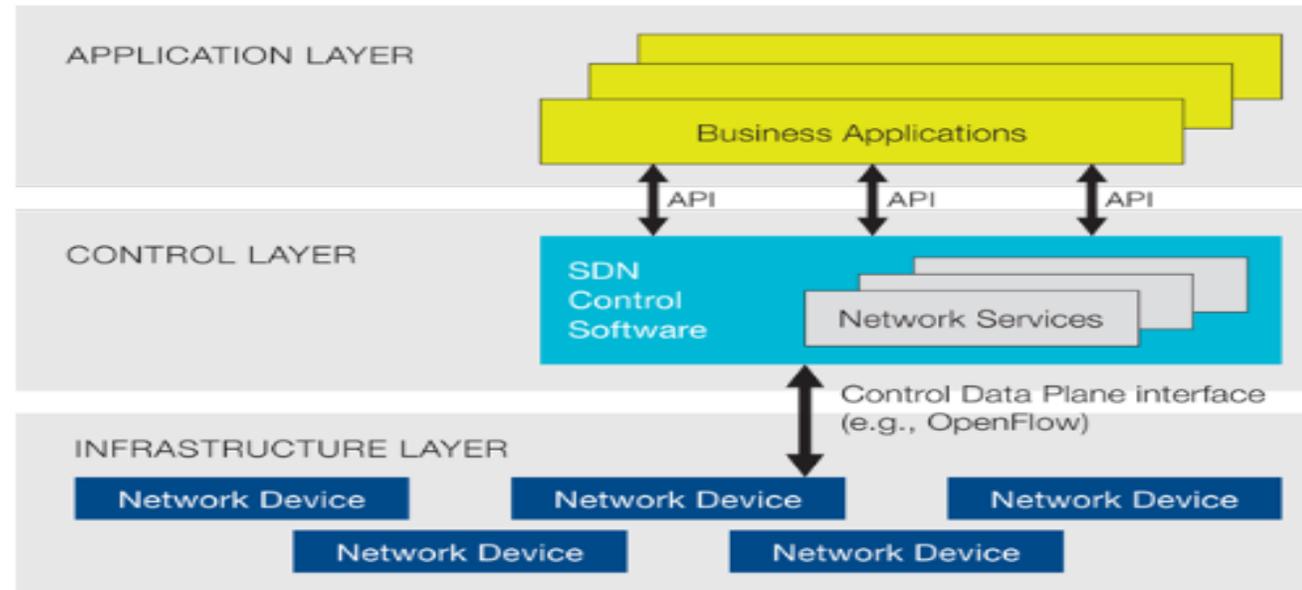
ОСНОВЫ SDN

- Программно определяемые сети (SDN)?

Новая архитектура, обеспечивающая прямое программирование сетей, основанных на отделении плоскости управления от плоскости данных.

- Достоинства SDN:

- Гибкость и взаимозаменяемость.
- Централизованное управление.
- Программирование сети.
- Динамичное управление приложениями.
- Основаны на открытых стандартах и не зависят от реализаций конкретных производителей.



Источник: Open Networking Foundation

ОСНОВЫ NFV

Виртуализация сетевых функций (NFV)

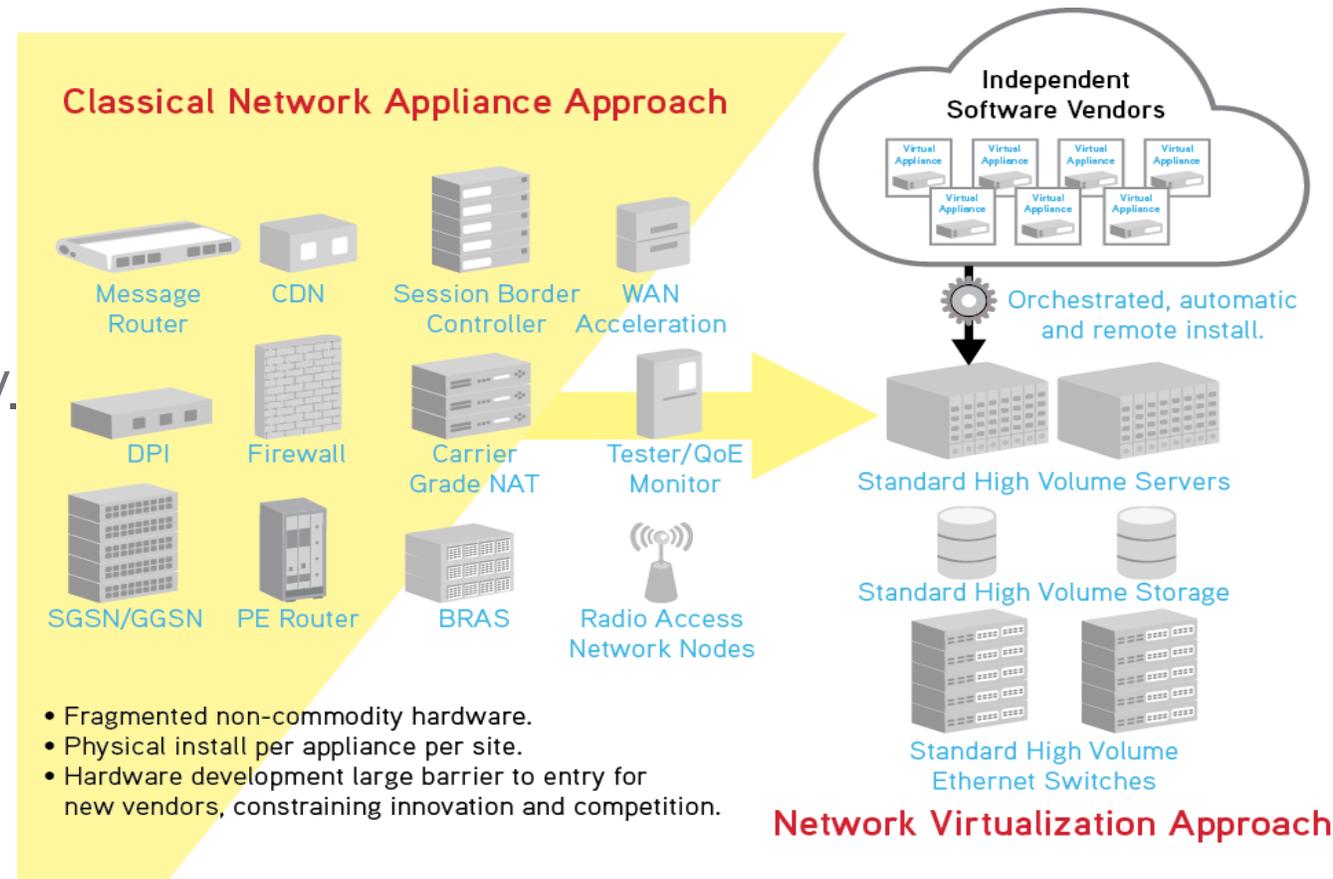
- Реализация сетевых функций на стандартных массовых серверах, коммутаторах и системах хранения данных.

ETSI Industry Specification Group (ISG)

- Определяет структуру и стандарты NFV.

Достоинства of NFV:

- Снижение CAPEX и OPEX.
- Гибкость и эластичность.
- Ускорение вывода на рынок.
- Повышение операционной эффективности.
- Новшества в виде ПО.



SDN & NFV

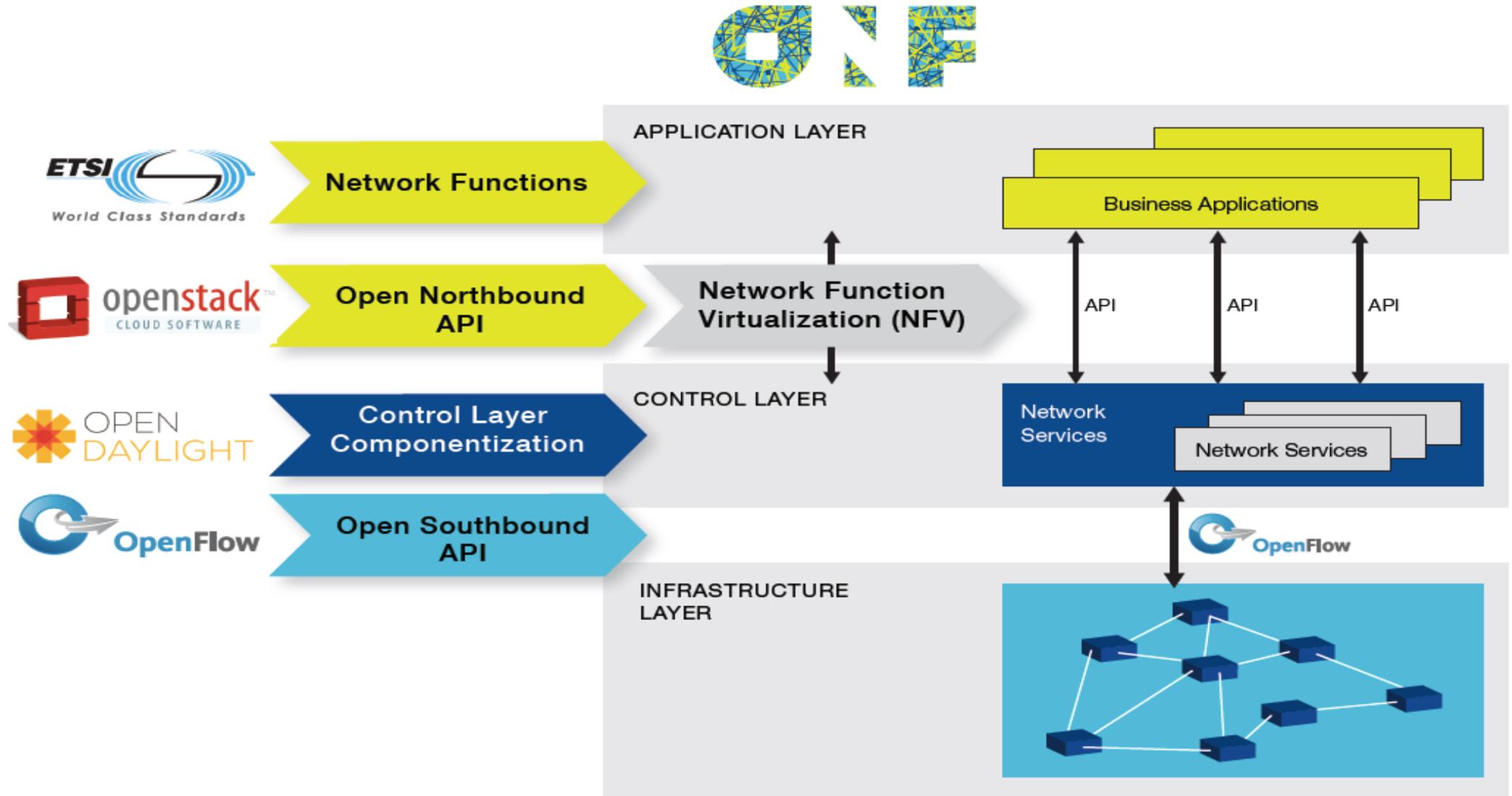
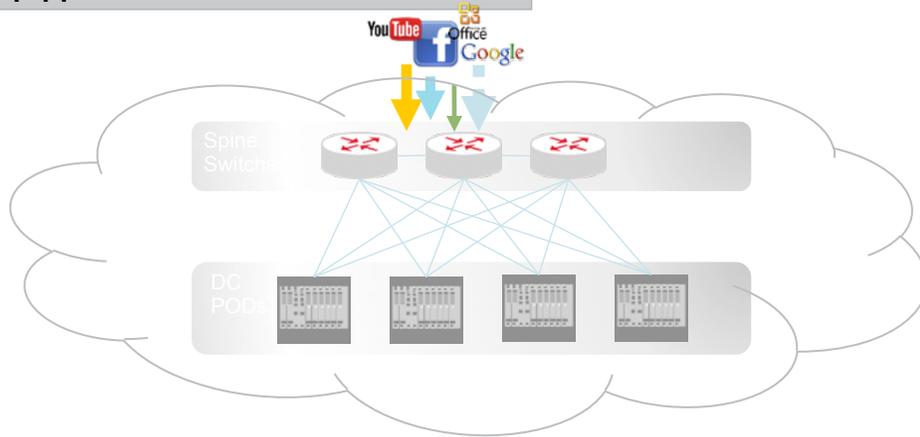


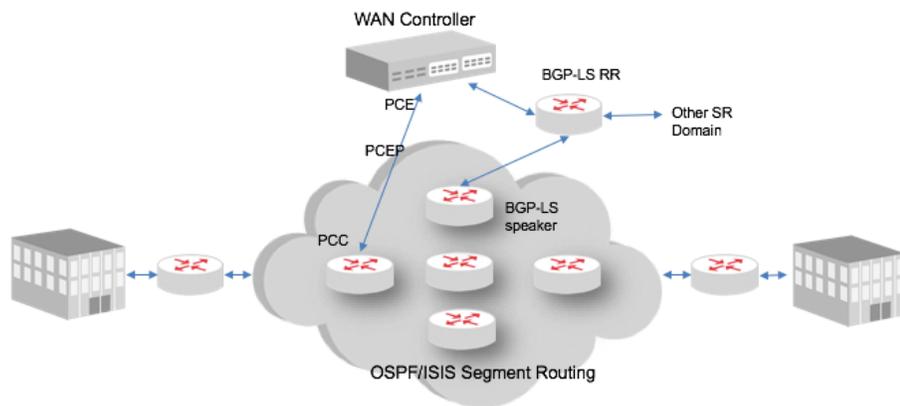
FIGURE 2: NFV and SDN Industry Map

ПРИМЕРЫ SDN

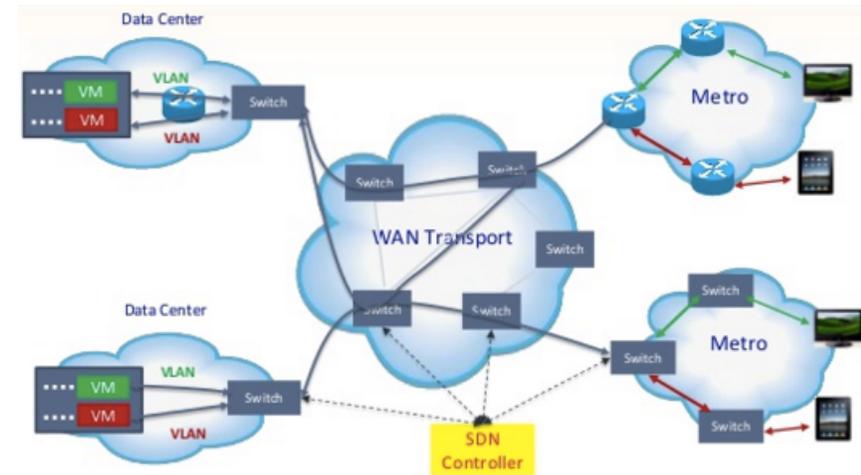
Сеть в гипермасштабируемом ЦОДе



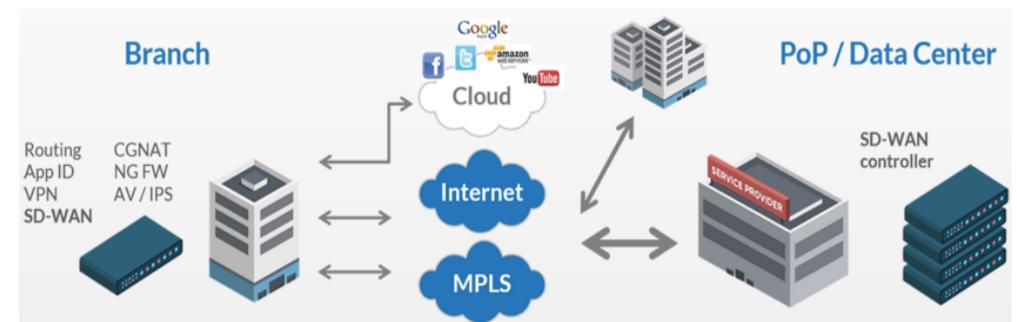
Операторская SDN



SDN-транспорт



Управляемая WAN



The logo for ixia is displayed on a 3D light blue cube. The text 'ixia' is in a white, lowercase, sans-serif font. The 'i' has a small red horizontal bar above it, and the 'x' has a small blue horizontal bar above it. The cube is positioned on the left side of the frame, casting a shadow on the surface below it.

ixia

**РЕШЕНИЯ ДЛЯ
SDN И NFV**

РЕШЕНИЯ ДЛЯ ТЕСТИРОВАНИЯ СЕТЕВЫХ ИНФРАСТРУКТУР

Гипермасштабируемый ЦОД

Гипермасштабируемость, высокая производительность и большое число портов.

Поддержка высокочастотной торговли, буферизация микровсплесков трафика.

Мультискоростные порты 100/40/10G, поддержка 100G QSFP28 с 4 x 25G

SDN

Поддержка моделей SDN overlay и underlay.

Определение производительности и масштабируемости SDN.

Проверка скорости переконфигурирования.

Виртуализированные сети и функции

Виртуализированные тестовые функции на базе VM и облаков.

Возможность тестирования физических и виртуальных сетевых инфраструктур.

Определение производительности виртуализированных сетевых функций.

Опорные сети следующего поколения

Охват всех протоколов и технологий.

Проверка масштабируемости операторского уровня и выполнения SLA.

Поддержка 100G CFP4.

IxNetwork

QuickTests

IXNETWORK – ТЕСТИРОВАНИЕ СЕТЕВЫХ ИНФРАСТРУКТУР И УСТРОЙСТВ



Платформы

- 12-слотовая XG12-SD
- 2-слотовая XGS2-SD
- IxNetwork Virtual Edition



Интерфейсы для тестирования

- Ethernet 1/10/25/40/100/400G
- BroadRReach Automotive Ethernet

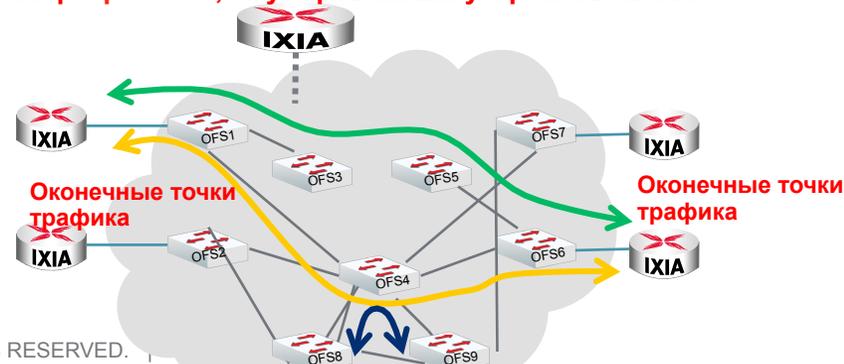


Технологии

- Маршрутизация IPv4/v6, Bridging, Broadband, Multicast, MPLS VPN
- Carrier Ethernet, Hyper Scale Data Center, SDN
- AVB/Automotive Ethernet

- Проверка SLA и эластичности сети для гипер-масштабируемых ЦОДов.
- Производительность, масштабируемость и плотность портов операторского класса.
- Полный набор тестов SDN и виртуализации сети.
- Автоматизация тестирования без сценариев, выдача профессиональных отчетов.

Контроллер OpenFlow, эмулированный устройством Ixia



- Первичный
- Вторичный
- Виртуальный

ТЕСТИРОВАНИЕ SDN

- ✓ Проверка соответствия коммутатора спецификации OpenFlow с помощью IxANVL

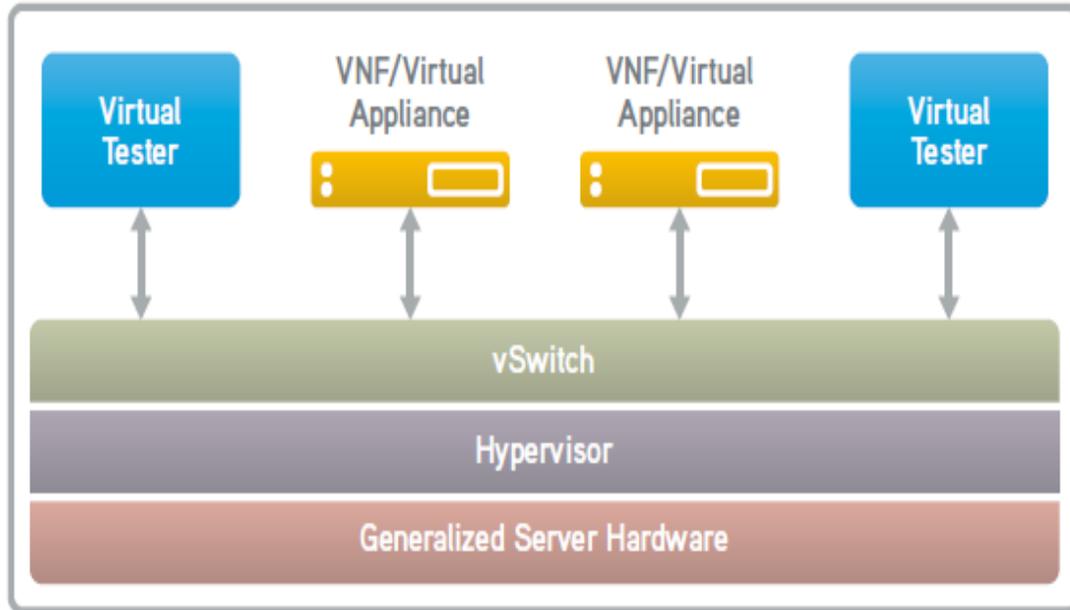


- ✓ IxNetwork Emulation
 - ✓ OpenFlow
 - ✓ VxLAN
 - ✓ EVPN/PBB-EVPN
 - ✓ Segment Routing
 - ✓ PCEP, BGP-LS
- ✓ IxNetwork QuickTest
 - ✓ Емкость таблицы потоков OF
 - ✓ Скорость запоминания адресов L2/3
 - ✓ Сходимость потока OF в случае сбоя

ТЕСТИРОВАНИЕ VNF И ЦЕПОЧКИ СЕРВИСОВ

(Сверху вниз)

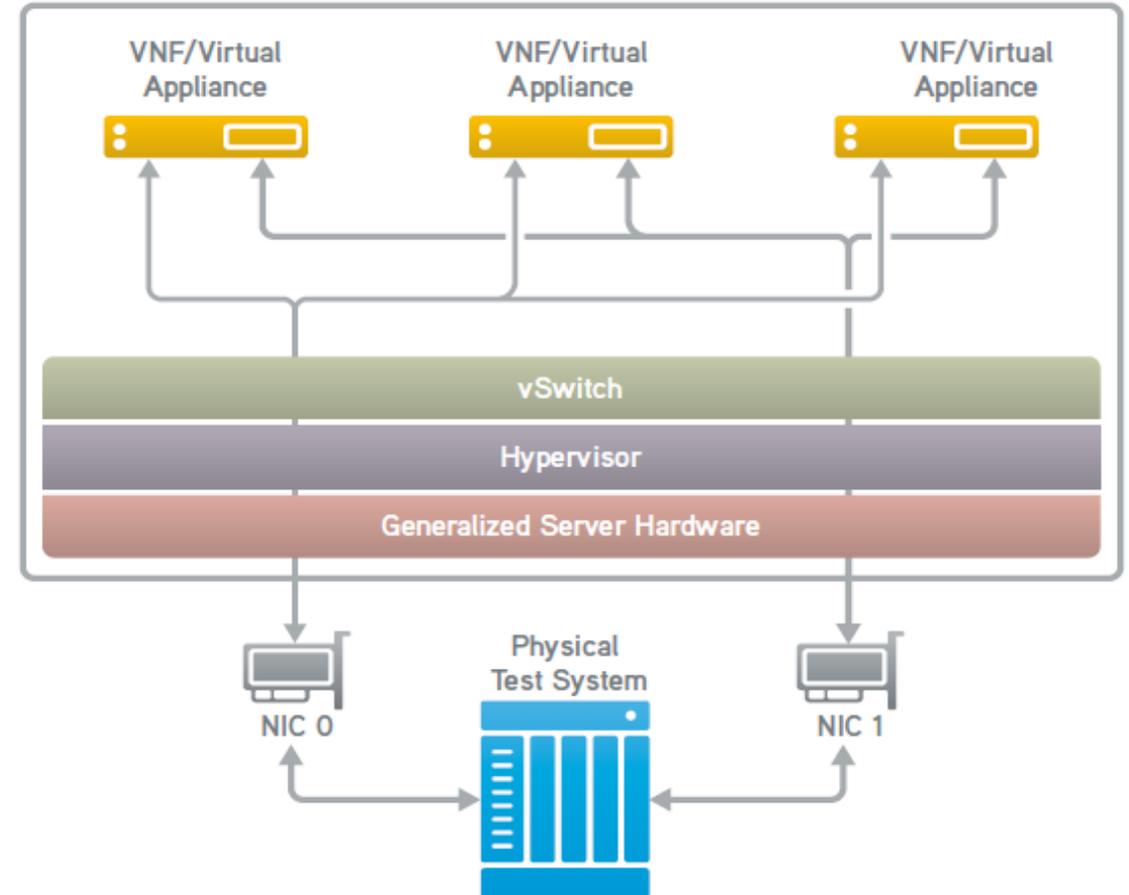
Generic Test Setup for Testing a Virtualized Network Using Virtualized Test Simulations



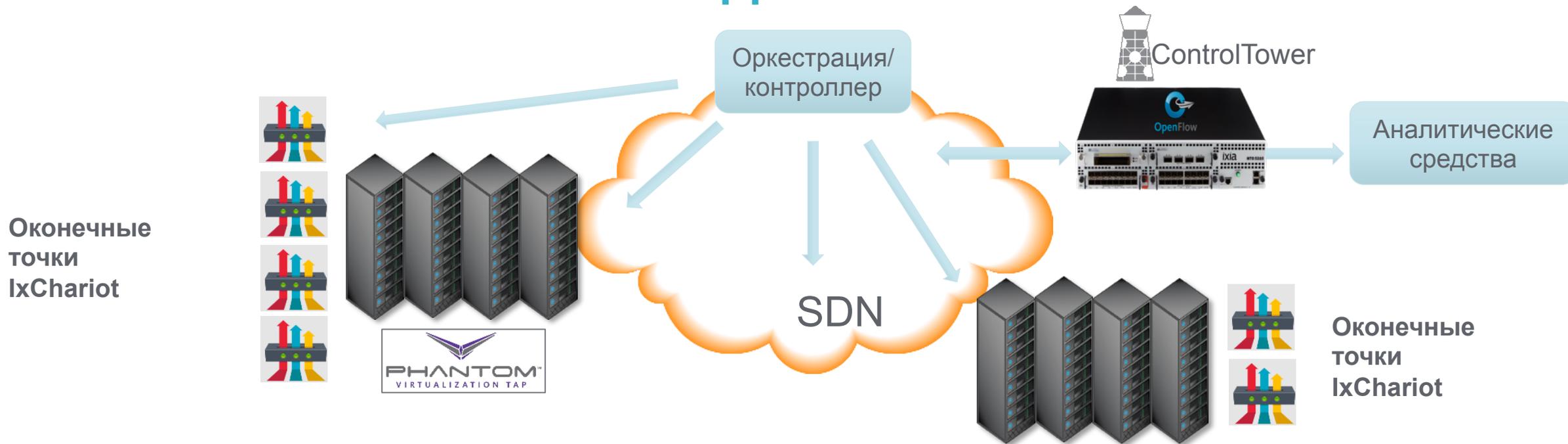
Note: Simulations may or may not be residing on the same hardware platform (server)

(Снизу вверх)

Generic Test Setup for Testing a Virtualized Network Using a Hardware-based Test Solution



ТЕСТИРОВАНИЕ SDN В ДЕЙСТВИИ



- Оценка работы действующей SDN с помощью IxChariot и HawkEye.
 - Оркестрация устанавливает оконечные точки IxChariot.
 - Определение KPI сервисов по всему маршруту передачи трафика (end-to-end) для проверки сетевой инфраструктуры, вычислительных возможностей и цепочек услуг.
- Архитектура мониторинга ControlTower для гибридных сетей.
 - Хорошо масштабируемая инфраструктура мониторинга с коммутаторами OpenFlow.
- Phantom vTap для контроля трафика в виртуализированной инфраструктуре.

НАШИ РЕШЕНИЯ

- Высокопроизводительные платформы для тестирования:
 - сетевых инфраструктур (включая SDN) на L2 и L3;
 - производительности приложений;
 - устойчивости к кибератакам;
 - мобильности.
- Определение производительности и безопасности виртуальных сетевых функций (VNF):
 - IxNetwork (VE),
 - IxLoad (VE),
 - BreakingPoint (VE).
- Оценка работы решений SDN и NFV до и после развертывания с помощью IxChariot и IxChariot Pro.
- Решения для контроля трафика на базе Phantom vTap.

IxChariot

Phantom vTap

BreakingPoint

VE

IxNetwork

VE

IxLoad

VE

The logo for ixia is displayed on a 3D light blue cube. The text 'ixia' is white, with a red dot above the 'i' and a blue dot above the 'i'.

ixia

**ОБЩЕОТРАСЛЕВАЯ
ДЕЯТЕЛЬНОСТЬ**

IXIA В ONF

Председатель и активный член рабочей группы Testing and Interoperability Working Group

- Занимается вопросами тестирования соответствия стандартам, совместимости и производительности.
- Развивает методику тестирования производительности решений на базе OpenFlow.

AppFest и PlugFest ONF – тестирование совместимости решений разных производителей.

- Активное участие в ежегодных AppFest и PlugFest.
- Первый PlugFest ONF – в Ixia iSimCity.



OPEN NETWORKING
FOUNDATION



Ixia в ETSI и OPNFV

ETSI NFV ISG

Член NFV ISG,
участник реализаций различных PoC NFV.

PoC#1: CloudNFV Open NFV Framework -
Accelerated Open Virtual Switch.

PoC#21: Network Intensive and Compute
Intensive Hardware Acceleration.

PoC#28: SDN Controlled VNF Forwarding
Graph.

Активный участник разработки нескольких
документов рабочей группы TST:

- NFV-TST001 Pre-Deployment testing



Open Platform for NFV (OPNFV)

Ixia – участник нескольких проектов:

- Yardstick – тестовая среда для проверки выполнения требований к инфраструктуре.
- Qtip – проект по тестированию производительности платформы.

Ixia участвует в:

- Тестировании производительности vSwitch для телекоммуникационных проектов NFV.
- Тестировании функциональности базовых систем (варианты применения vEPC).

ТЕСТИРОВАНИЕ СОВМЕСТИМОСТИ РЕШЕНИЙ РАЗНЫХ ПРОИЗВОДИТЕЛЕЙ В EANTC – 2016 MPLS+SDN+NFV WORLD CONGRESS

Ethernet VPN

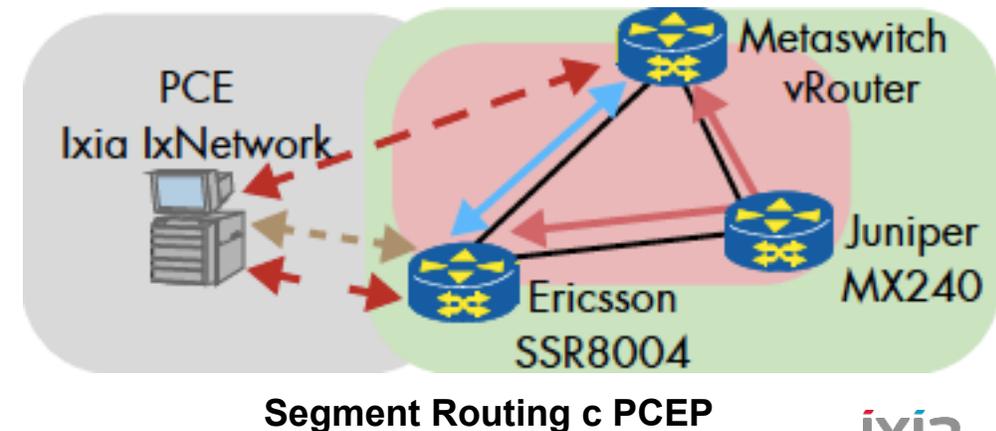
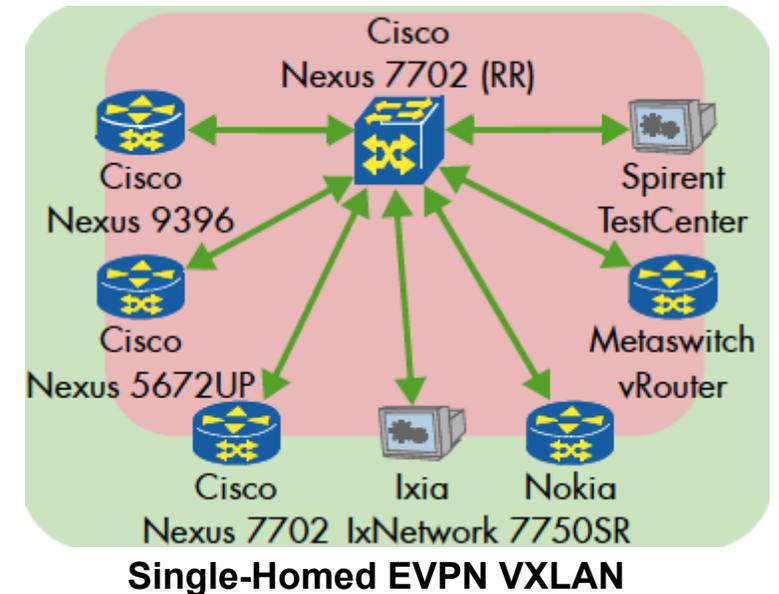
- Успешно продемонстрированы все разновидности EVPN : EVPN, PBB-EVPN, EVPN VXLAN.
- Совместимость с решением основных производителей.

Segment Routing

- Успешно продемонстрировано расширение Segment Routing для IGP.

PCEP и BGP-LS

- Успешно продемонстрировано установление пути PCE Segment Routing.



Арег Алимян,

старший директор по маркетингу продуктов, Ixia

Тел: +1.818.268.2199

Email: aalimian@ixiacom.com



**WE MAKE
APPLICATIONS
STRONGER**