ARBOR NETWORKS

Концепция защиты от DDoS-атак

Антон Шевчук

+7.967.285.85.72

ash@netwell.ru

Arbor Networks – кто это?

Производитель, которому доверяют защиту своих сетей самые крупные и требовательные бизнесы мира

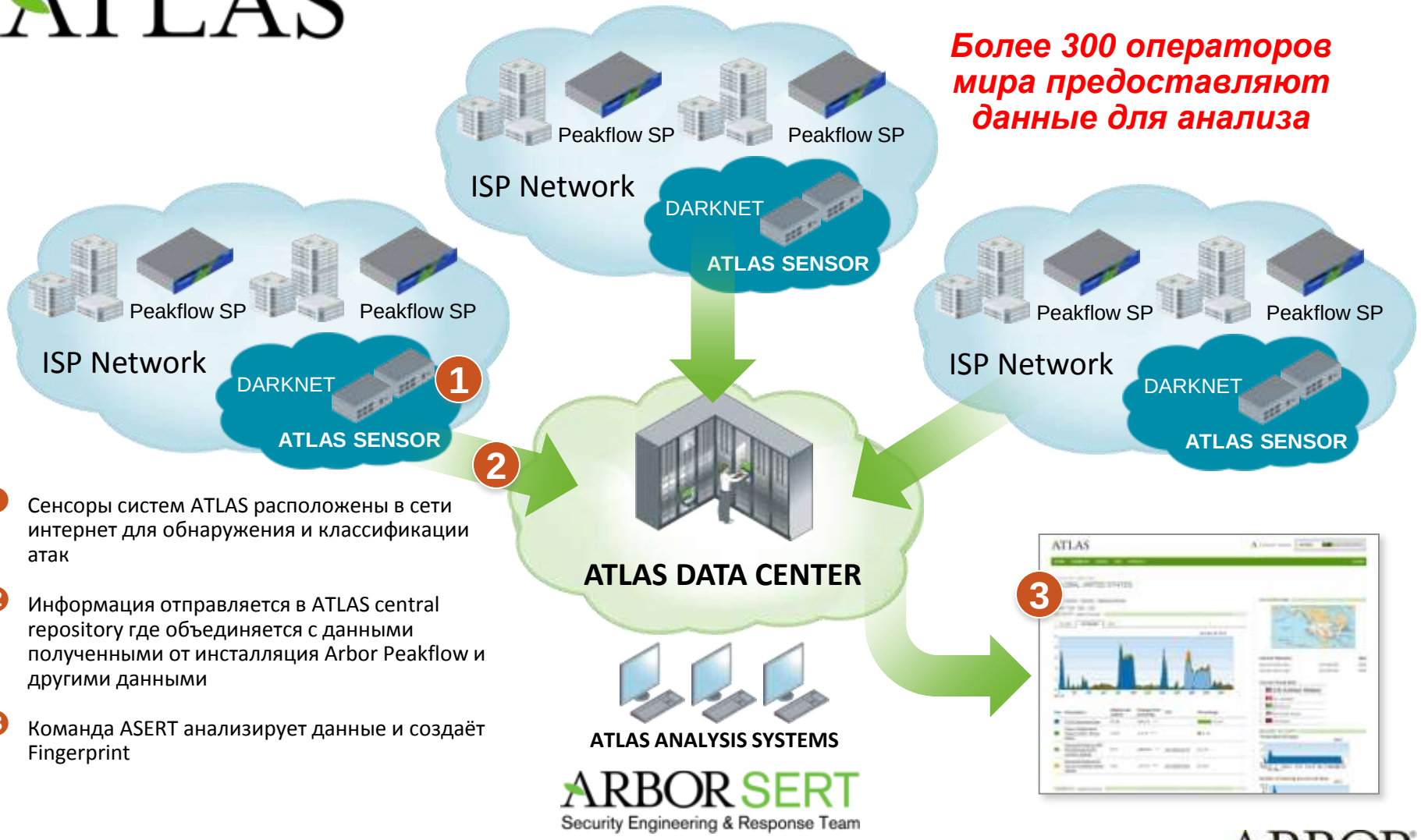
100%	Процент Tier 1 операторов, являющихся клиентами Arbor 
#1	Защищает крупнейший сети компании и наиболее значимые мировые события. Последнее событие мирового масштаба под защитой Arbor Networks – Олимпийский игры в Сочи 2014.
140+ Тб/с	Трафик, отслеживаемый системой ATLAS в данный момент – ***Это почти треть всего Интернет трафика.***
#1	Позиция Arbor на рынке оборудования защиты от DDoS в сегментах Carrier - 54%, Enterprise – 50%, Mobile – 48% [Infonetics Research декабрь 2015]
16 лет	Arbor Networks поставляет инновационные продукты и технологии по обеспечению безопасности и мониторинга сетей с 2000 года

Active Threat Level Analysis System (ATLAS)

ATLAS®

Первая в мире система анализа угроз

Более 300 операторов мира предоставляют данные для анализа

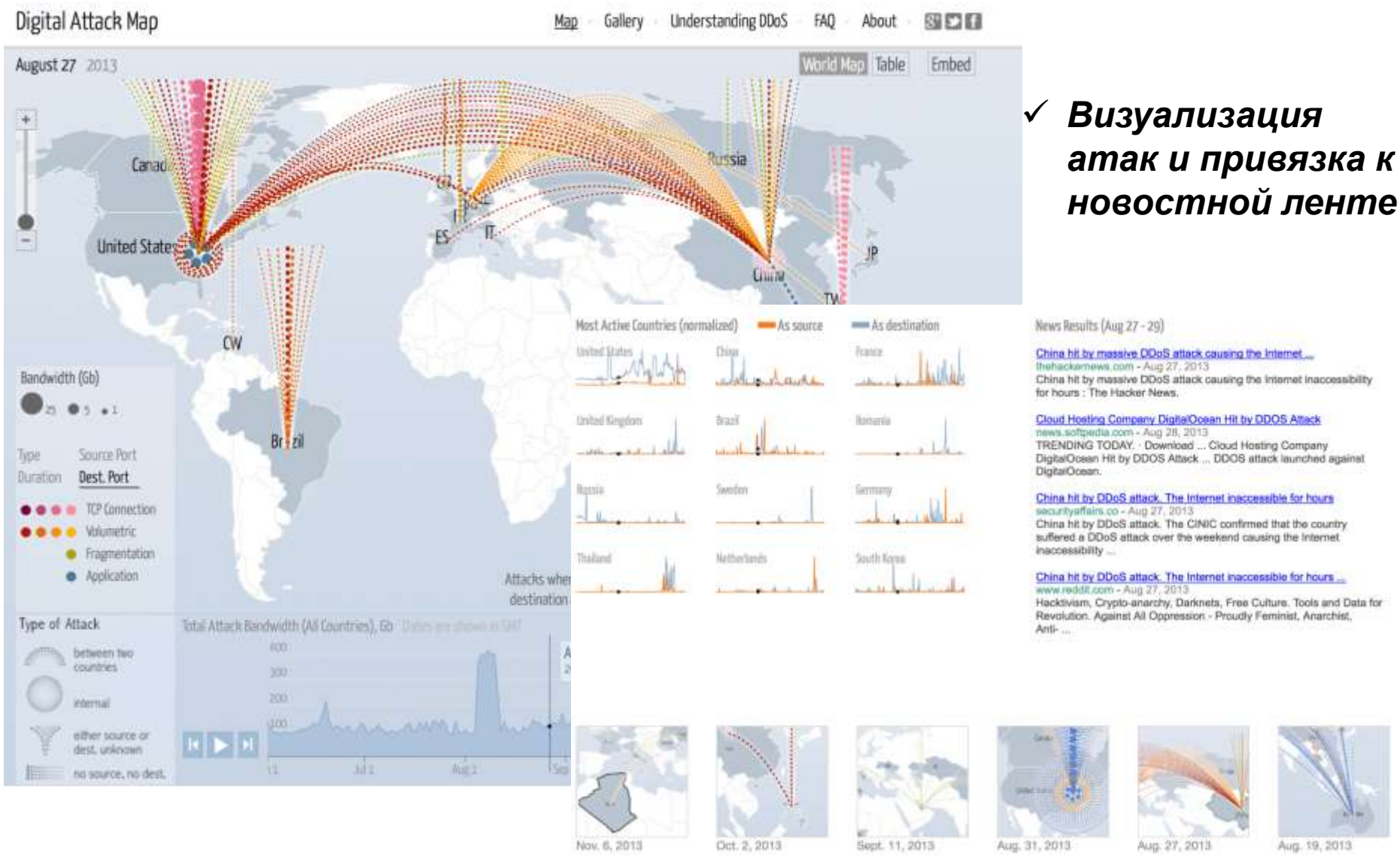


1. Сенсоры систем ATLAS расположены в сети интернет для обнаружения и классификации атак
2. Информация отправляется в ATLAS central repository где объединяется с данными полученными от инсталляция Arbor Peakflow и другими данными
3. Команда ASERT анализирует данные и создаёт Fingerprint

ARBOR NETWORKS

ATLAS and Google

Digital attack map http://www.digitalattackmap.com/



- ✓ ***Визуализация атак и привязка к новостной ленте***

ARBOR NETWORKS

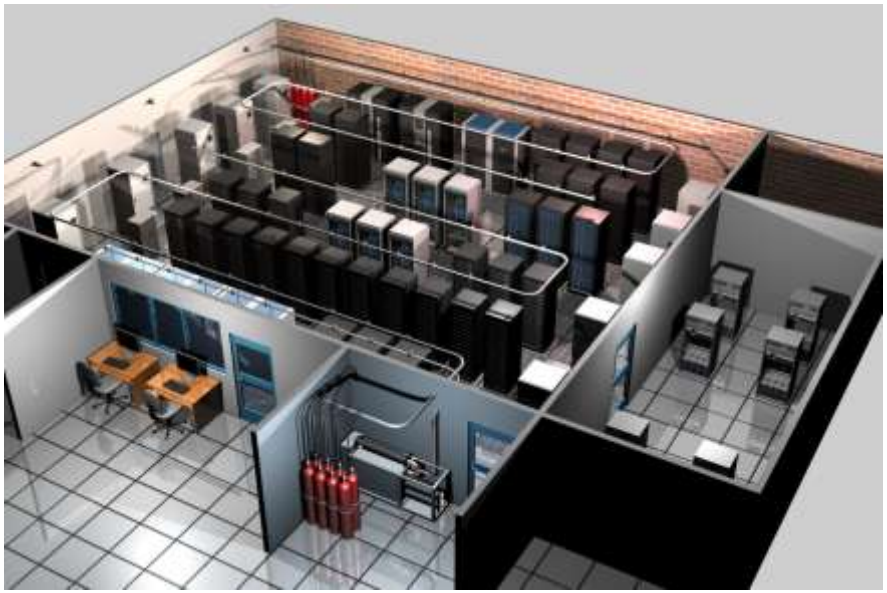
Современная инфраструктура

Многие компании создают узлы связи:

- Бесперебойное электропитание
- Автоматическая система пожаротушения
- Высоклассные и отказоустойчивые системы охлаждения
- Современная высокопроизводительная сетевая инфраструктура
- Превосходное серверное оборудование
- Получение сертификаций на обеспечение доступности, например Uptime Institute Tier III/Tier II/Tier I

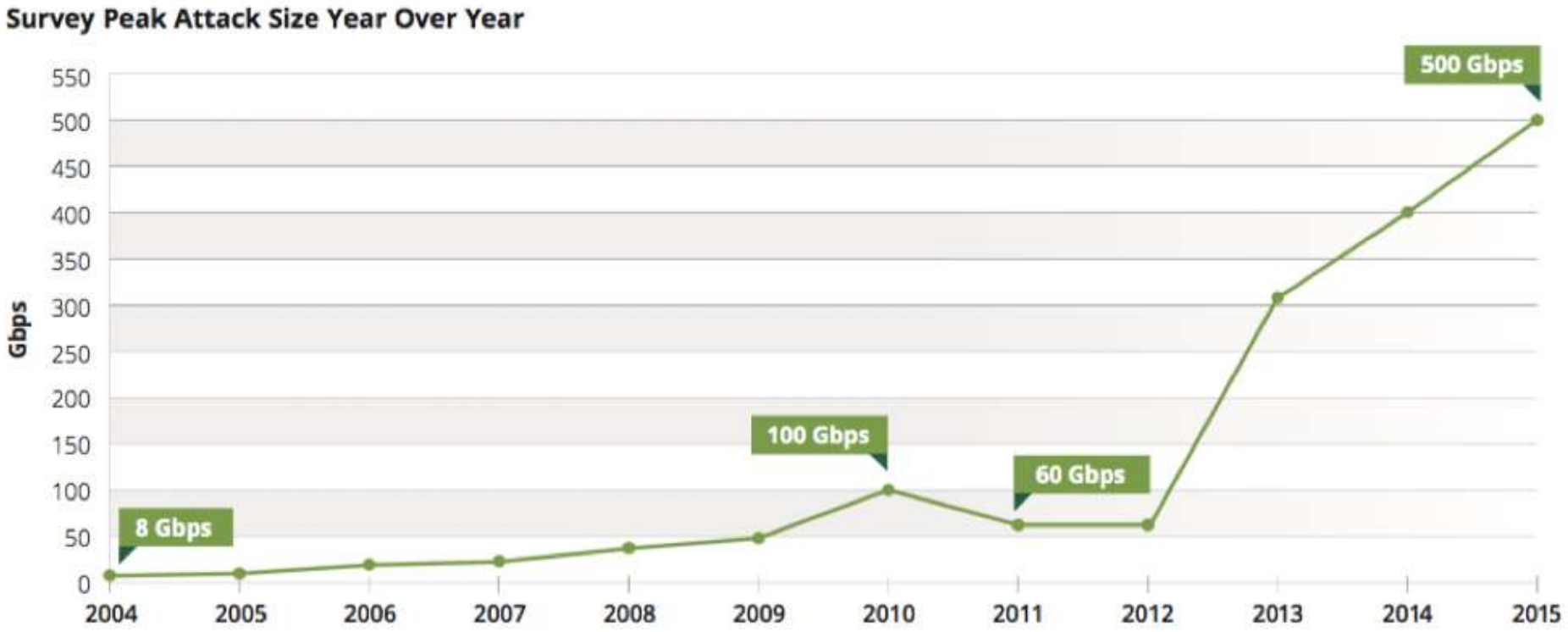
Но поможет ли это при:

- **Малозаметных** атаках на приложения (Application attack)?
- Атаках на **инфраструктуру сетевой безопасности**?
- При атака типа **переполнения канала** связи?
- Сможете ли вы понять **кто вас атаковал** и когда были атаки на протяжении времени?
- Можете ли вы точно сказать - **взламывали** ли вас или нет?



ARBOR NETWORKS

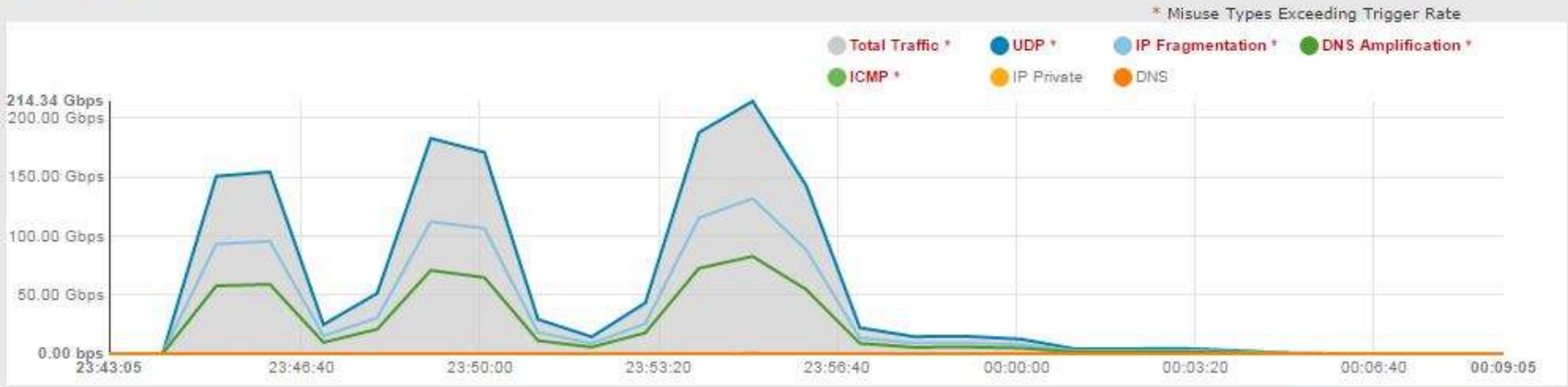
Ddos атаки становятся все больше



ARBOR NETWORKS

В России в 2016 году

Alert Traffic



Top Traffic Patterns (last 5 minutes)

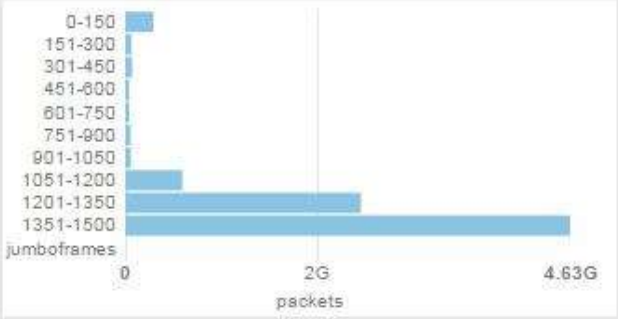
Download All Patterns

No patterns found in the last 5 minutes of the selected timeframe.

Alert Characterization

Misuse Types	Total Traffic (7)	100.00%
Destination IP Addresses		100.00%
Source IP Addresses	Highly Distributed	99.00%
Protocols	udp (17)	99.00%
Misuse Types	UDP (9)	99.00%
Destination UDP Ports	0	61.00%
Source UDP Ports	0	61.00%
Misuse Types	IP Fragmentation (1)	61.00%
Source UDP Ports	53 (domain)	38.00%
Destination UDP Ports	4444 (nv-video)	36.00%
Source Countries	Russian Federation	29.00%

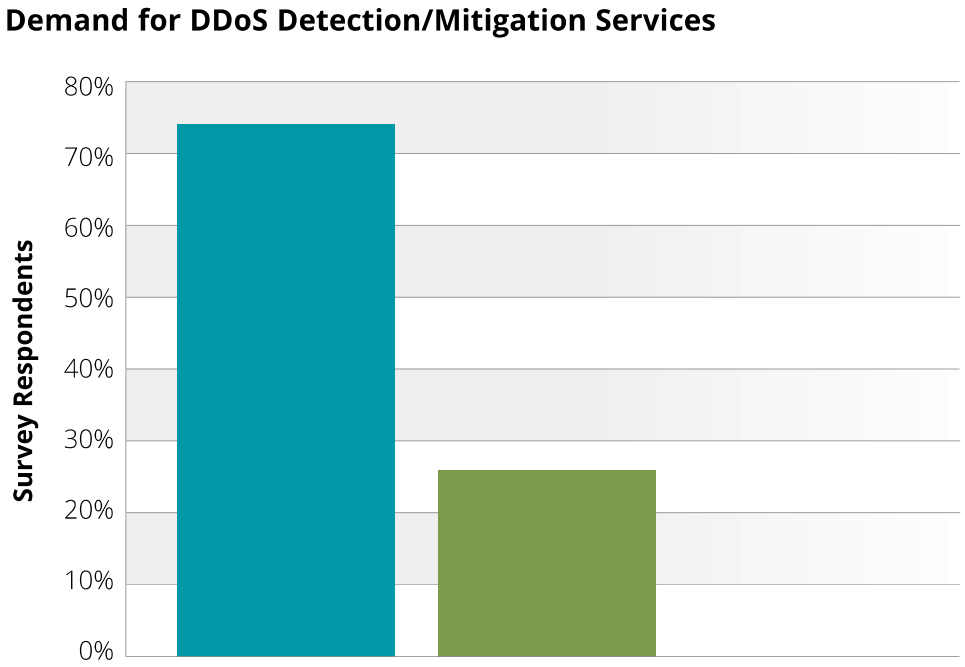
Packet Size Distribution



Крупнейшая атака в России на сети Ростелеком в 214.234 Gbps

ARBOR NETWORKS

Спрос на защиту растет



- **74%** Increasing demand from customers
- **26%** The same demand from customers
- **0%** Reduced demand from customers

53% Корпоративных заказчиков испытали сбой сети из-за DDoS атак на межсетевые экраны и устройства IDP/IPS

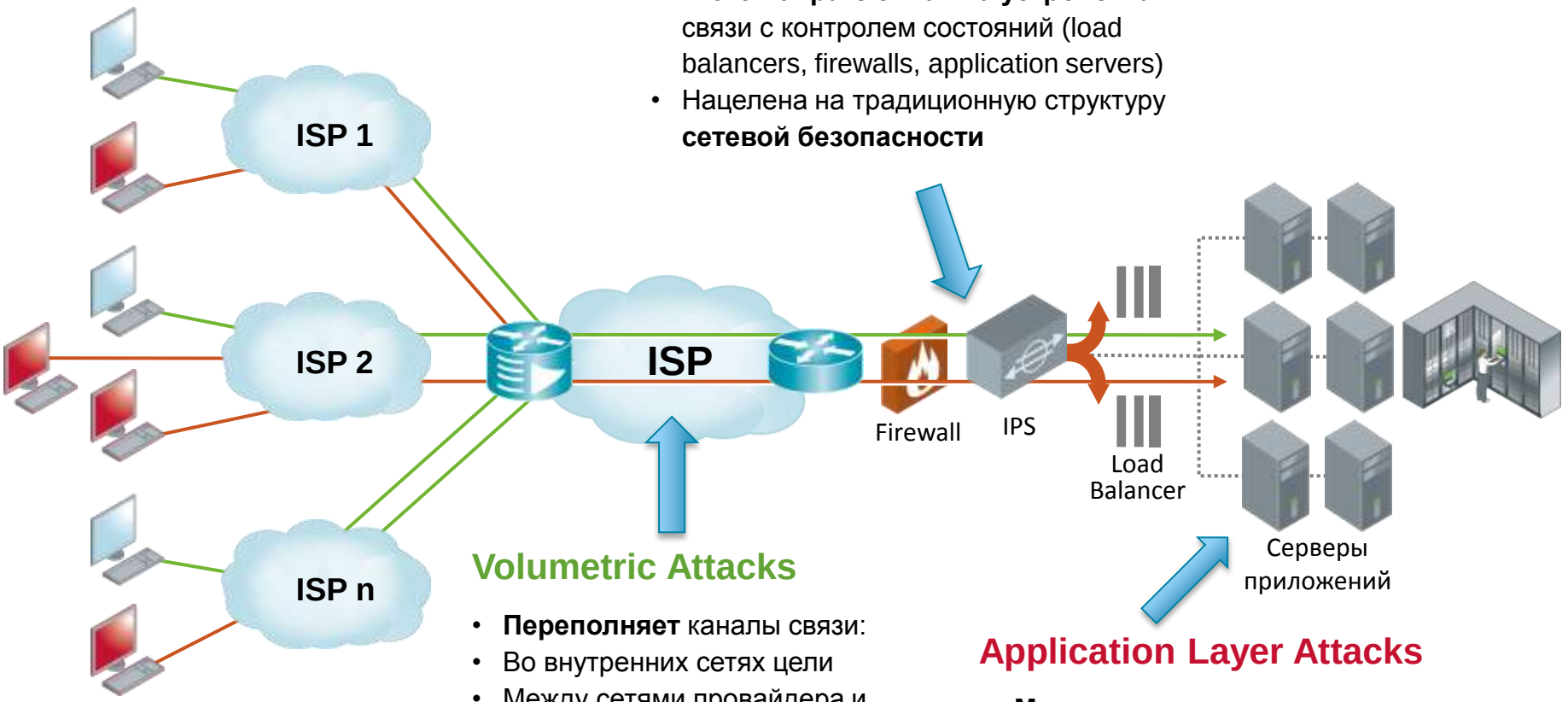
ARBOR NETWORKS

Анатомия DDoS-атак. Что такое DDOS?

Как и какие части сетевой инфраструктуры атакуют?

TCP State-Exhausting Attacks

- Атака **направленная на устройства** связи с контролем состояний (load balancers, firewalls, application servers)
- Нацелена на традиционную структуру **сетевой безопасности**



Volumetric Attacks

- **Переполняет** каналы связи:
- Во внутренних сетях цели
- Между сетями провайдера и атакуемой сетью

Application Layer Attacks

- **Малозаметные** атаки на приложения
- Нацелены на определённые уязвимости приложений

ARBOR NETWORKS

Решение для защиты - Arbor APS

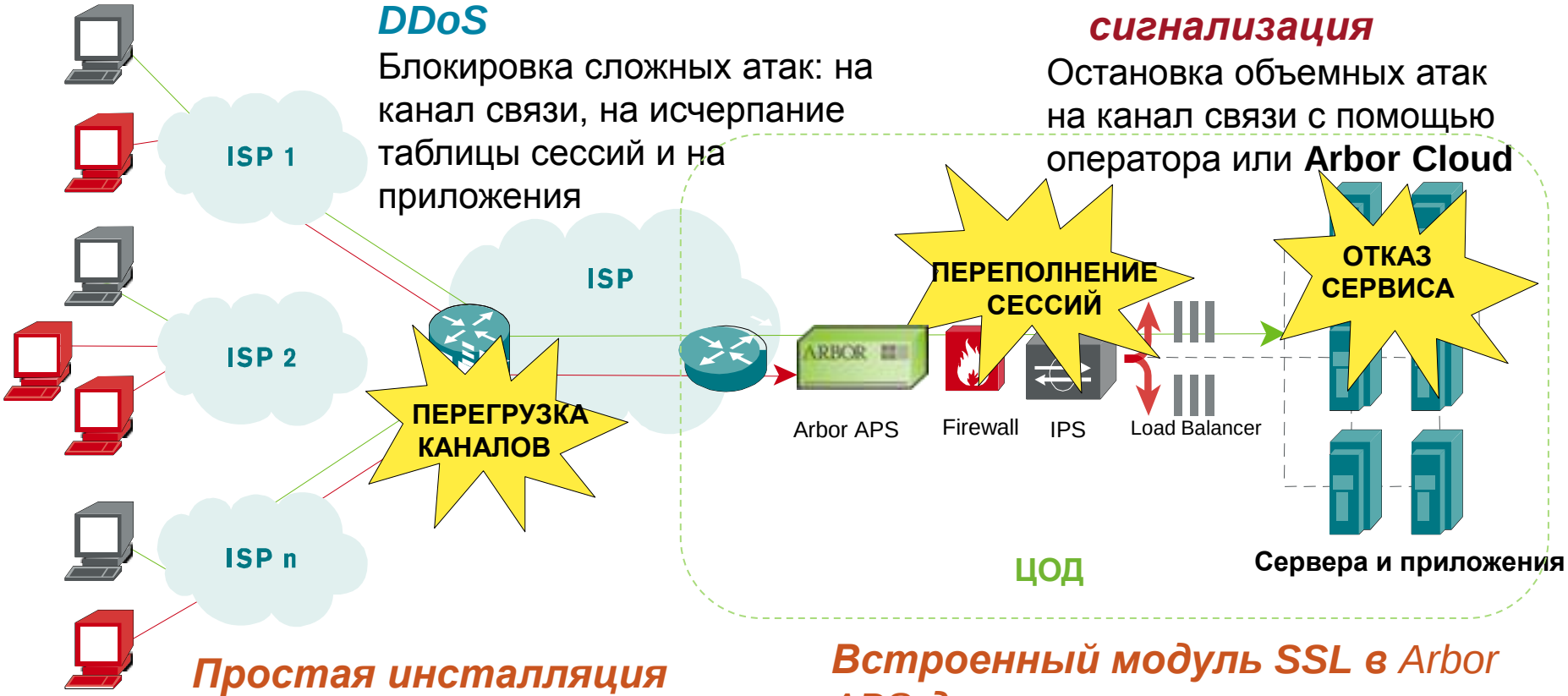
Проверенная защита от DDoS атак на площадке клиента

Блокировка сложных DDoS

Блокировка сложных атак: на канал связи, на исчерпание таблицы сессий и на приложения

Облачная сигнализация

Остановка объемных атак на канал связи с помощью оператора или **Arbor Cloud**



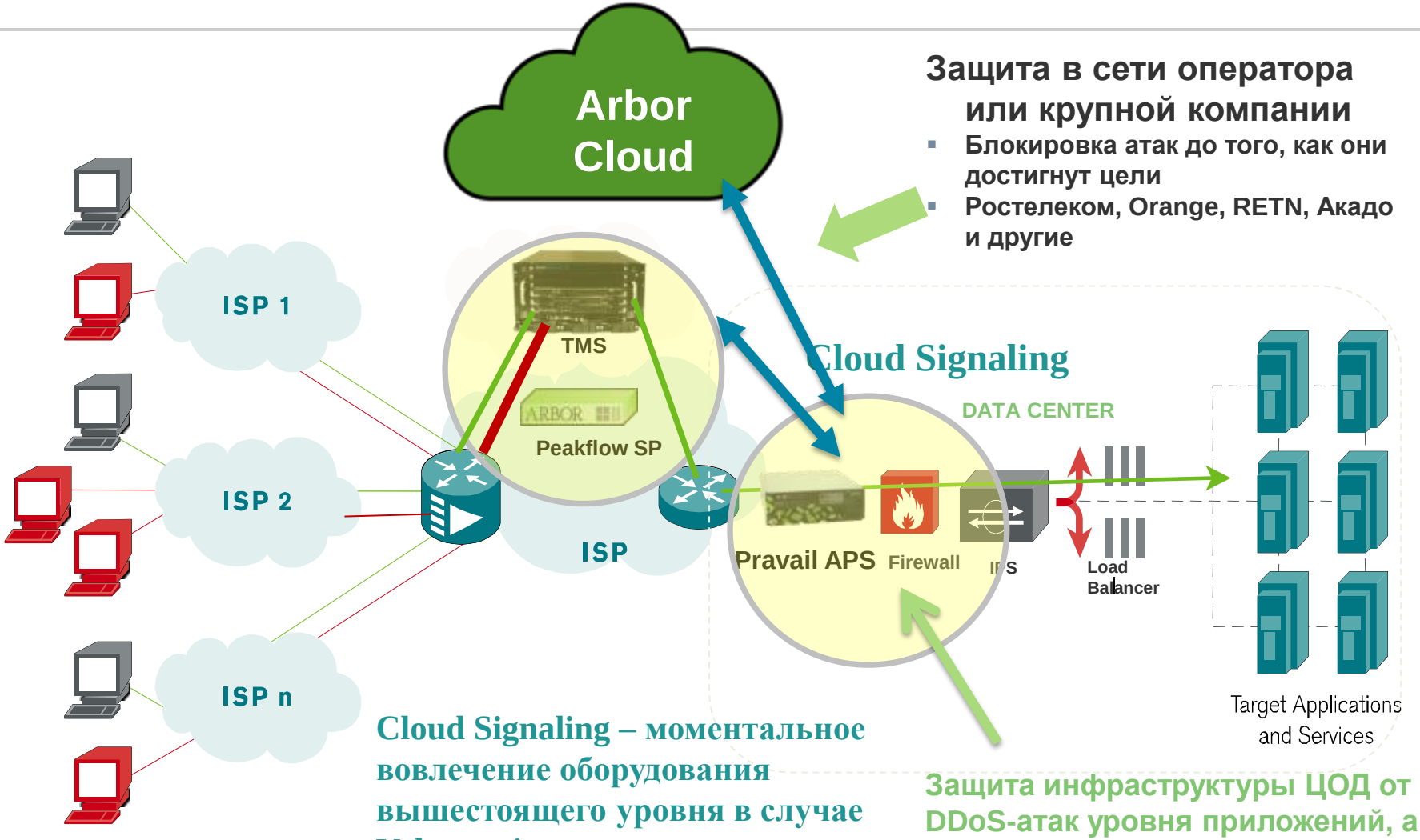
Простая инсталляция

Автообновление сигнатур останавливает актуальные угрозы

Встроенный модуль SSL в Arbor APS для остановки атак на сервисы с использованием шифрования

ARBOR NETWORKS

Эшелонированная защита от Arbor Networks



Защита в сети оператора или крупной компании

- Блокировка атак до того, как они достигнут цели
- Ростелеком, Orange, RETN, Акадо и другие

Cloud Signaling – моментальное вовлечение оборудования вышестоящего уровня в случае Volumetric атаки

Защита инфраструктуры ЦОД от DDoS-атак уровня приложений, а также от Volumetric до установленного порога, в том числе и для митигации атак с использованием SSL

A Recommended Industry Best Practice:

FORRESTER® IDC FROST & SULLIVAN Infonetics RESEARCH Securosis ovum

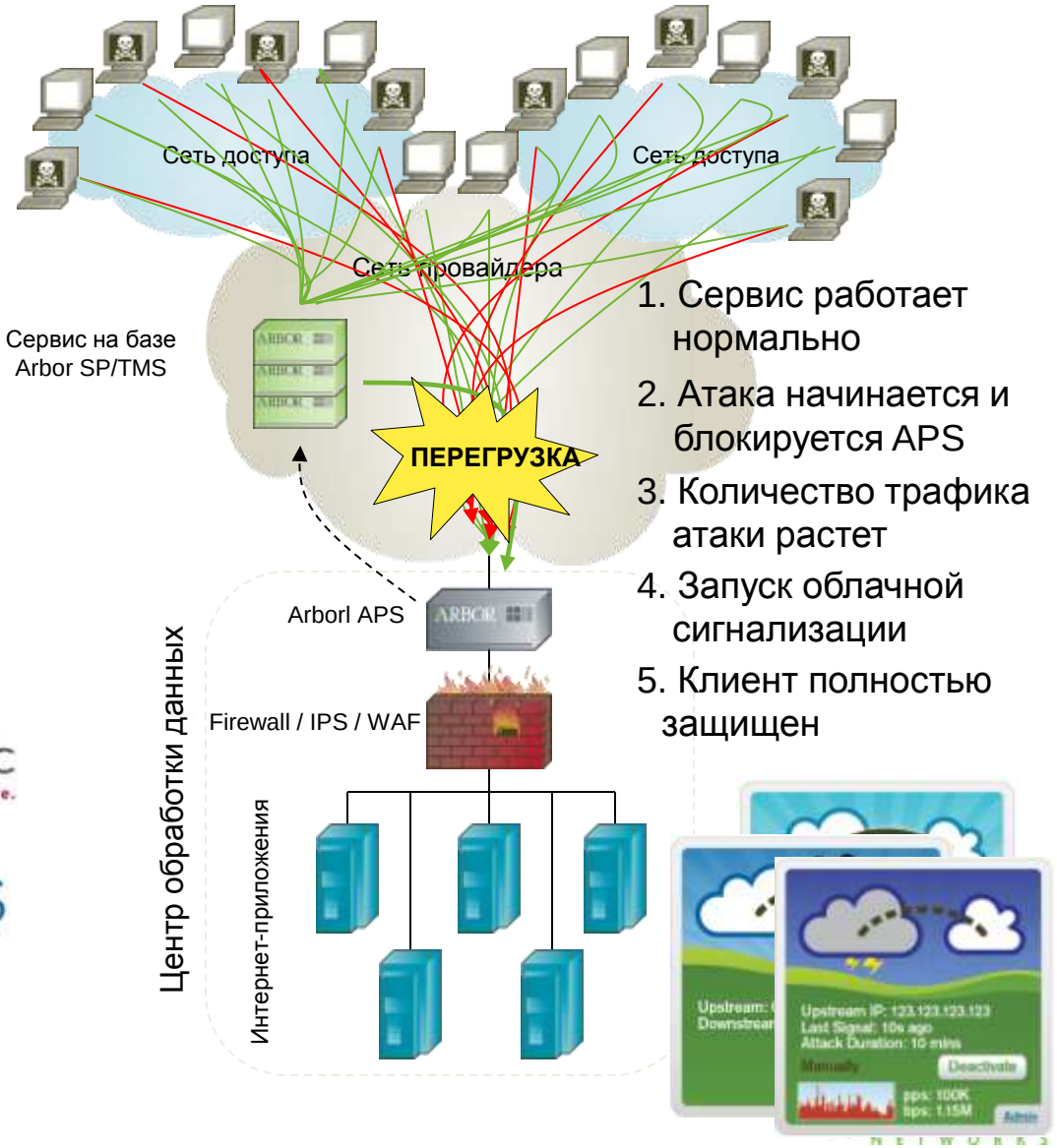
ARBOR NETWORKS

Альянс Cloud Signaling

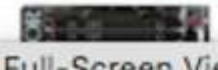
CLOUD SIGNALING COALITION

Сотрудничество ISP и их клиентов с помощью протокола облачной сигнализации.

adversor DDoS Protection That Works™ · AXtel Comunícate mejor. · aixit · circular · colt smarter / faster / further · du وحيا بها الحياة add life to life · Embratel · TATA · PROLEXIC DDoS Attacks End Here. · Telefónica · TelstraClear · VOCUS communications · swisscom · neustar



Доступные платформы Arbor в 2016 году

Platform	Traffic Inspection Capacity	Blocking Capacity	Connection Options	Size
vmware KVM	100 Mbps – 1+ Gbps	1+ Gbps	any	any
 TMS 2300/APS 2600	500 Mbps – 20 Gbps	20 Gbps	1/10 GE	2U
 TMS/APS 2800	10 Gbps – 40 Gbps	40 Gbps	1/10 GE	2U
 Full-Screen View TMS 5000	25 – 100 Gbps	400 Gbps	10/40/100 GE	6U
 TMS HD1000	20 Gbps - 160 Gbps	160 Gbps	10 GE	2U

ARBOR NETWORKS

Где можно посмотреть наши решения?

- **О DDOS атаках**
  - The Evolution of DDoS Attacks http://www.youtube.com/watch?v=Q7deVOUXPFk
  - Различные материалы о DDOS http://www.arbornetworks.com/resources/media-library
  - Записанные вебинары, в том числе о решениях: http://www.arbornetworks.com/resources/media-library/enterprise-webinars
- **Система Atlas**
  - DDoS Attack Protection: Arbor Network's ATLAS http://www.youtube.com/watch?v=0U68W6gTkP8
  - Atlas Dashboard http://atlas.arbor.net
- **О нашей команде Asert**
  - Arbor Networks: Researching DDoS and Advanced Threats http://www.youtube.com/watch?v=T3oBpvcBxD4
  - Worldwide Infrastructure Security report http://www.youtube.com/watch?v=-83m82sEpNI
  - DDoS and the Evolving Advanced Threat Landscape http://www.youtube.com/watch?v=92p_MbPbewk
  - Asert blog http://www.arbornetworks.com/asert/
- **Решения Arbor Networks (SP, APS, Spectrum, Arbor Cloud)**
  - Comprehensive DDoS Protection Solutions http://www.youtube.com/watch?v=JP299b-IG6g
  - Video about Pravail family solutions:http://www.youtube.com/watch?v=Qznv913qVzw&list=PLu8eXm-IEjEC-kbMOSsQKPJGoc1V75fnw
  - Spectrum Product Tour https://youtu.be/WOKT4Vd2LPQ
  - Cloud-Based DDoS Protection from Arbor Networks http://www.youtube.com/watch?v=kPJ-wjyhyoM

ARBOR NETWORKS

Спасибо за внимание!

Антон Шевчук

+7.967.285.85.72

ash@netwell.ru

WIRED

“Arbor Networks знает о работе Internet больше чем кто-либо еще. Если Вы хотите узнать, как выглядит актуальный профиль трафика и угроз в Интернете, взгляните на сервис ATLAS.»

ARBOR NETWORKS