

# Обзор продуктов Arbor Networks

Arbor APS / AED / SP / TMS

Максим Бузмаков  
системный инженер



# DDoS атаки 2020

- Только в 1 полугодии 2020 обнаружено 4.83 миллиона атак.
- Частота DDoS атак во время пандемии увеличилась +25%.
- Частота DDoS атак на операторов связи возросла до 492 807
- 15 новых reflection/amplification векторов были использованы в атаках с 2017 по 2020 год.
- Ожидаемый рост IoT до 20,4 миллиардов устройств в 2020 году.

▲ 25%

In DDoS attack frequency during pandemic lockdown



FREQUENCY  
492,807

DDoS attacks in  
the first half  
of 2020

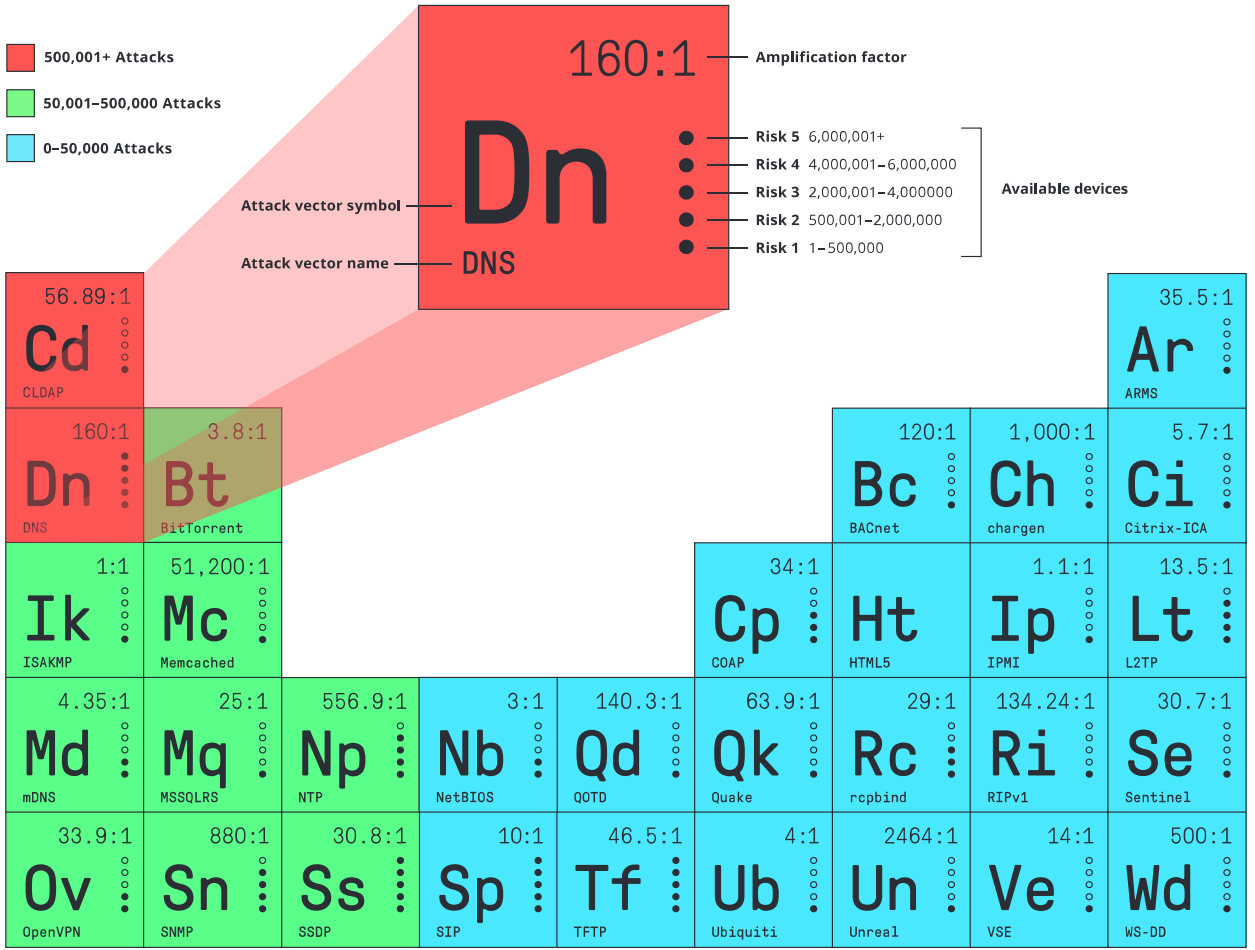
4,83M

**IoT: Botmaster's Dreams  
Come True**

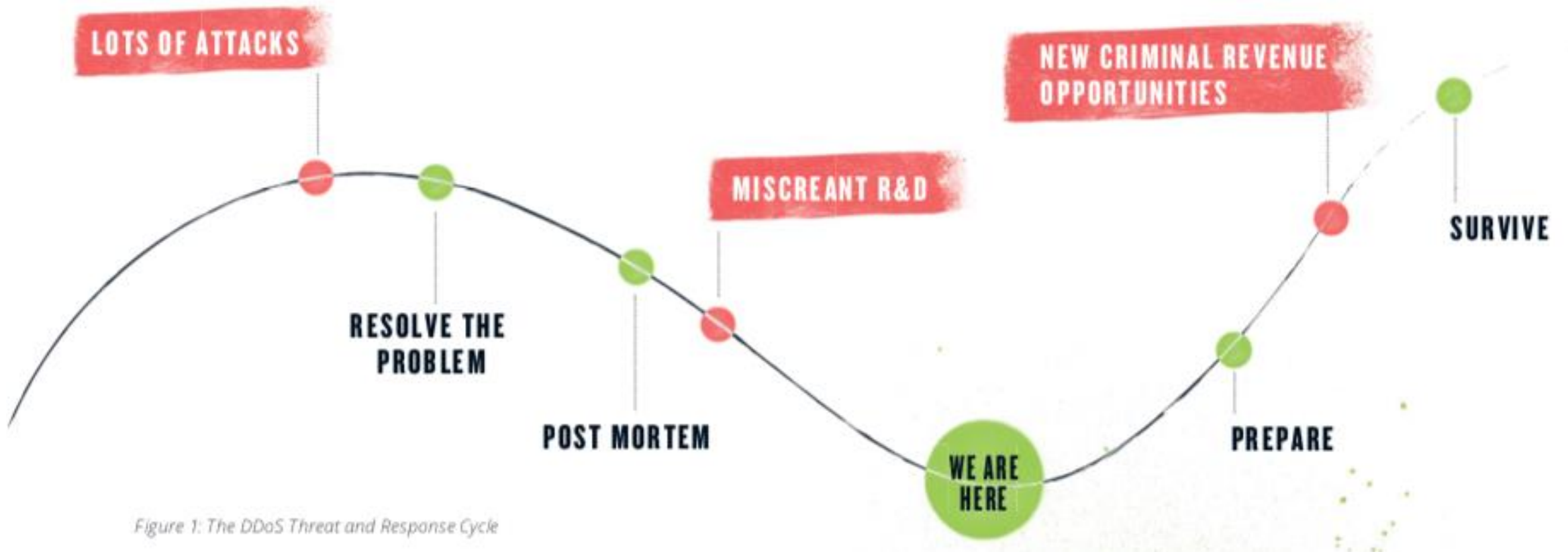
Devices forecast to  
connect to the  
internet in 2020

20,4B

# Ключевые элементы DDoS-атак



# DDoS атаки и Глобальные тренды



# Arbor – лидер в индустрии по защите от DDoS атак

19

Number of years Arbor has been delivering innovative security and network visibility technologies & products

98%

Percentage of world's Tier 1 service providers who are Arbor customers



#1

NETSCOUT Is 1<sup>st</sup> Place in Overall DDoS Prevention Appliance Market 22%



1<sup>st</sup> Place  
Transport  
18%



1<sup>st</sup> Place  
Data Center  
27%

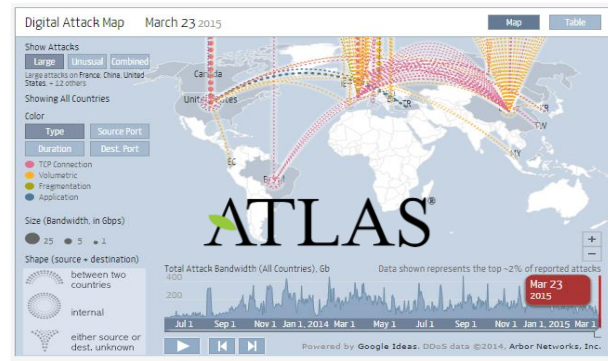


1<sup>st</sup> Place  
Mobile  
27%

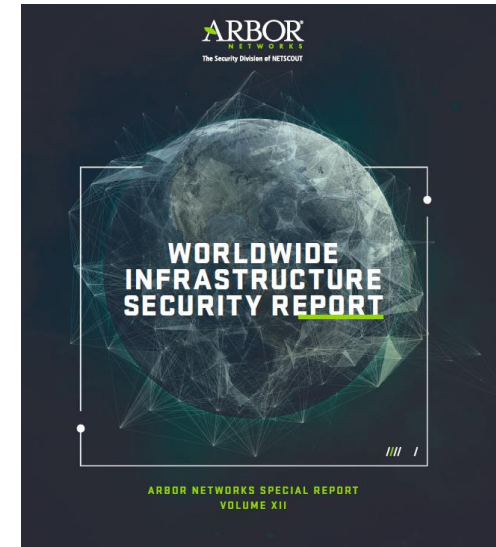
<https://omdia.tech.informa.com/>

1/3

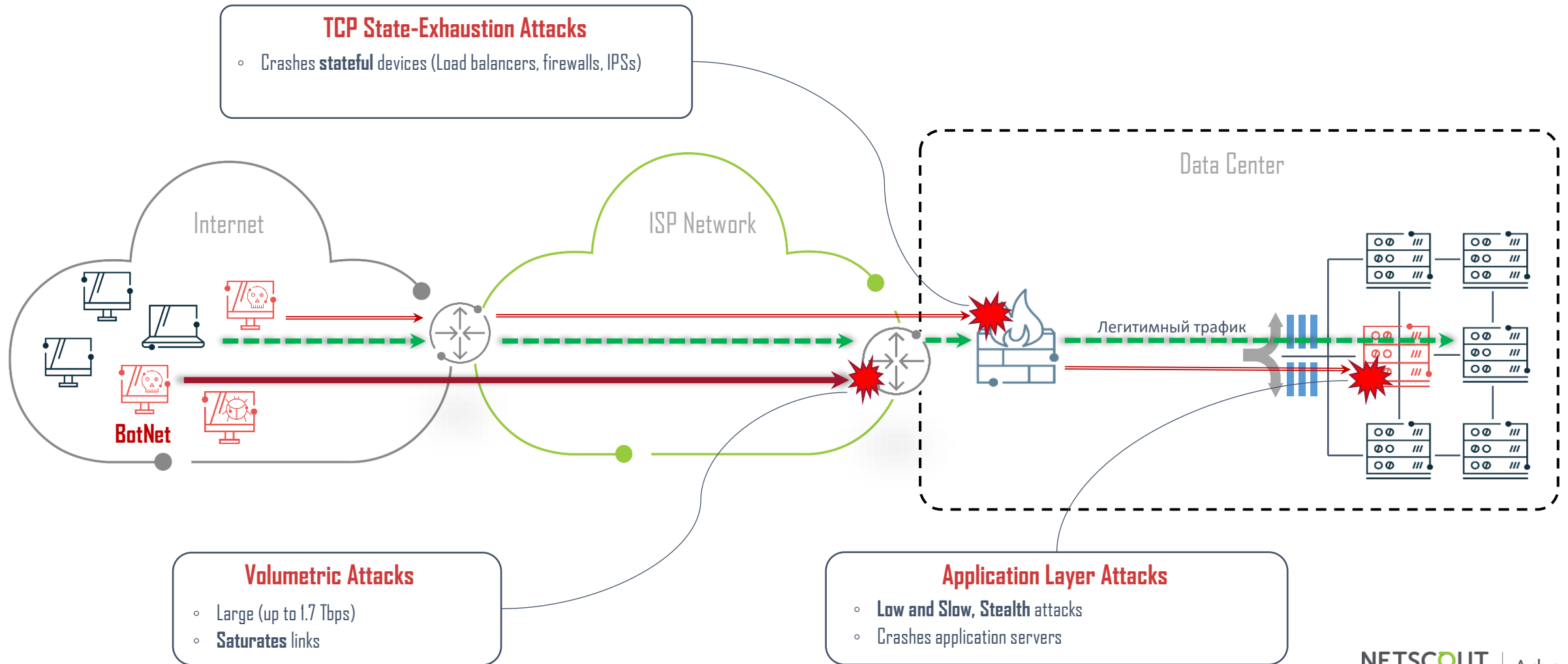
= Amount of Internet traffic monitored by the ATLAS



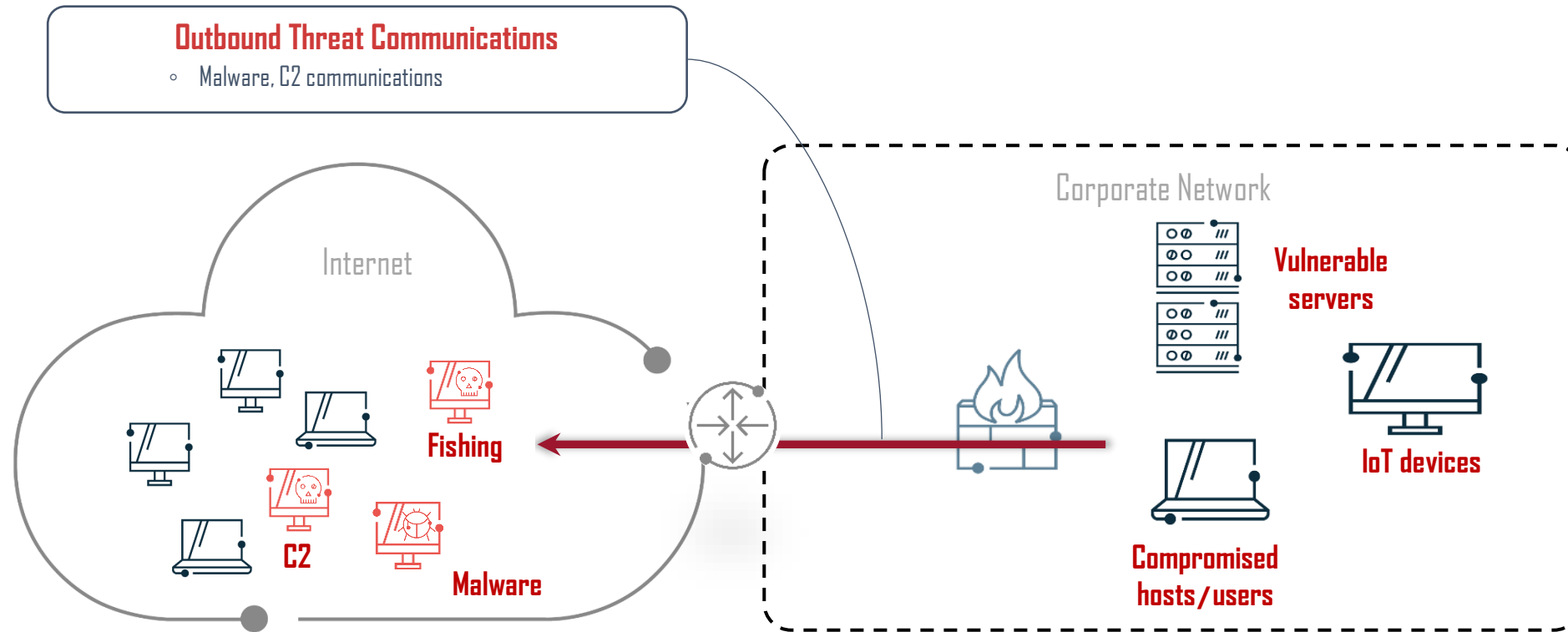
<http://digitalattackmap.com>



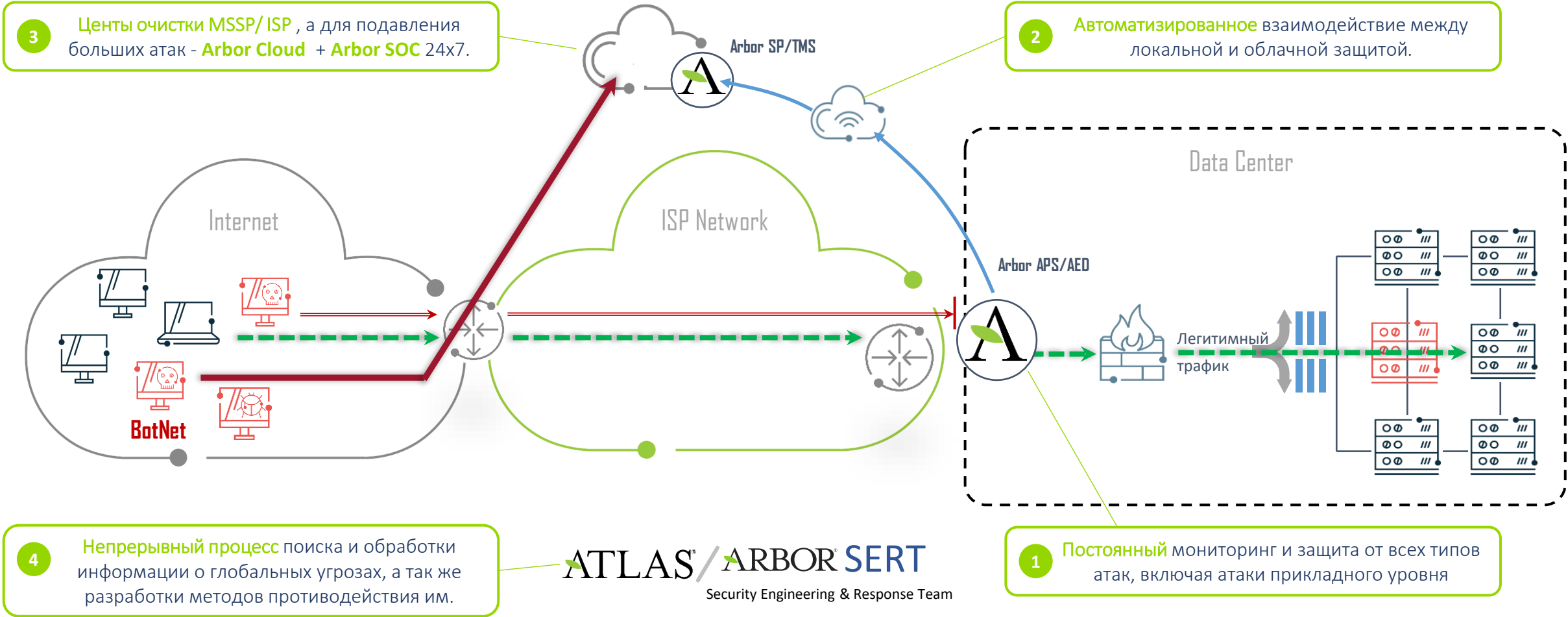
# Внешние угрозы - DDoS атаки



# Угрозы внутри периметра – Advanced Threats



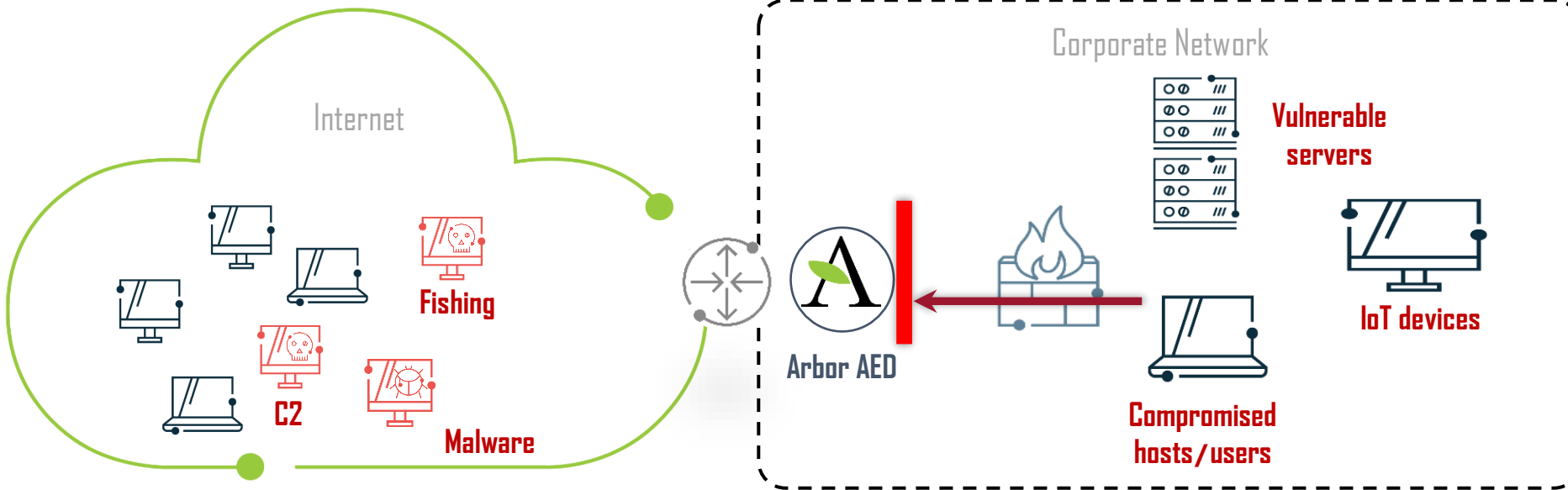
# Эшелонированная защита Arbor от DDoS атак





# Защита внутренних IT ресурсов

Блокировка с использованием IoC и репутационных баз данных об угрозах.



Непрерывный процесс поиска и обработки информации о глобальных угрозах, а так же разработки методов противодействия им.

ATLAS / ARBOR SERT  
Security Engineering & Response Team

# Arbor APS первая линия обороны

**Простое и быстрое** внедрение обеспечивается тем, что установка не требует изменения архитектуры сети (установка на периметре сети, перед NGFW), а для начала работы достаточно минимальной начальной конфигурации.

**Постоянный** мониторинг и защита от всех типов DDoS атак **Volumetric, Application** и **Resources exhaustion attacks** т.е. атак на истощение пропускной способности каналов, нацеленных на истощение ресурсов и атак прикладного уровня.

**Автоматизированное** взаимодействие между локальной и облачной защитой Arbor (Arbor Cloud/MSSP/ISP) с помощью **Cloud Signaling** позволяет предотвращать атаки, размер которыхкратно превосходит пропускную способность UPLINK интерфейсов.



# Arbor AED последний рубеж

**Постоянное** отслеживание и блокировка всех угроз как во входящем трафике **DDoS**, **Malware**, так и в исходящих сетевых соединениях к вредоносным ресурсам **C2**, **Malicious URLs** на основе IoC и уникальных данных об киберугрозах из базы ATLAS.

**Непрерывное** обновление информации о глобальных угрозах из ATLAS – ATLAS Intelligence Feeds (**AIF**) позволяет динамично реагировать и блокировать новые источники угроз, например центры управления ботнет сетями.



# Arbor APS 2600/2800

## APS 2600

### Платформа

- 2 x Intel Xeon E5-2608L v3 (6 cores)
- 32GB DDR
- RAID 2x120 SSD
- 2RU, AC/DC

### Лицензируемая производительность:

- 100Mbps, 250Mbps, 500Mbps,
- 1Gbps, 2Gbps, 5Gbps
- 10Gbps, 15Gbps, 20Gbps

### Сетевые интерфейсы:

- 4, 8 или 12x1GE с поддержкой Hardware Bypass
- 4 x 10GE, 4 или 8x1GE с поддержкой Hardware Bypass

### Дешифрация SSL/TLS:

- 750M HSM @ 750 Mbps
- 5G HSM @ 5 Gbps

## APS 2800

### Платформа

- 2 x Intel Xeon E5-2648L v3 (12 cores)
- 64GB DDR
- RAID 2x240 SSD
- 2RU, AC/DC

### Лицензируемая производительность:

- 10Gbps, 20Gbps, 30Gbps и 40Gbps

### Сетевые интерфейсы:

- 8 или 8x10GE с поддержкой Hardware Bypass
- 4 x 1GE интерфейса с поддержкой Hardware Bypass

### Дешифрация SSL/TLS:

- 5G HSM @ 5 Gbps

# Arbor AED 2600/2800

## AED 2600

### Платформа

- 2 x Intel Xeon E5-2608L v3 (6 cores)
- 32GB DDR
- RAID 2x120 SSD
- 2RU, AC/DC

### Лицензируемая производительность:

- 100Mbps, 250Mbps, 500Mbps,
- 1Gbps, 2Gbps, 5Gbps
- 10Gbps, 15Gbps, 20Gbps

### Сетевые интерфейсы:

- 4, 8 или 12x1GE с поддержкой Hardware Bypass
- 4 x 10GE, 4 или 8x1GE с поддержкой Hardware Bypass

### Дешифрация SSL/TLS:

- 750M HSM @ 750 Mbps
- 5G HSM @ 5 Gbps

## AED 2800

### Платформа

- 2 x Intel Xeon E5-2648L v3 (12 cores)
- 64GB DDR
- RAID 2x240 SSD
- 2RU, AC/DC

### Лицензируемая производительность:

- 10Gbps, 20Gbps, 30Gbps и 40Gbps

### Сетевые интерфейсы:

- 8 или 8x10GE с поддержкой Hardware Bypass
- 4 x 1GE интерфейса с поддержкой Hardware Bypass

### Дешифрация SSL/TLS:

- 5G HSM @ 5 Gbps

# Arbor Virtual APS/AED

## vAPS/vAED

### Гипервизор

- VMware vSphere 5.5+
- KVM kernel 3.19 QEMU 2.0

### Поддержка Amazon AWS

- Да, Amazon EC2

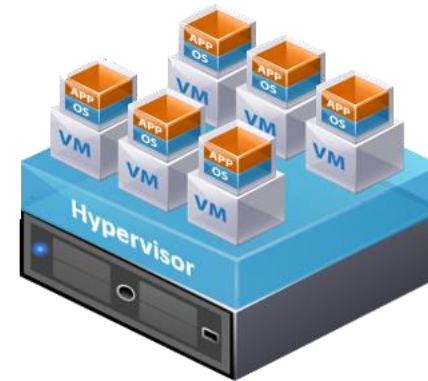
### Аппаратные требования:

- vCPUs: 1; NICs: 1 to 10; Memory: 6 GB; Storage: 100 GB

### Производительность на Instance:

- Пропускная способность при инспекции до 1 Gbps
- Максимальная скорость потока DDoS до 600 Kpps

## Virtual Appliances



Pre-installed  
Pre-configured  
OS & App Stack



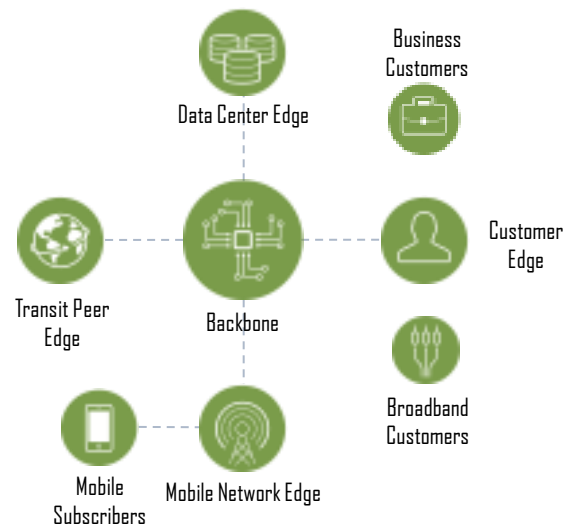
# Arbor SP = контроль сети

**Визуализация** пирингового, транзитного и магистрального трафика, а так же возможность мониторинга трафика клиентов на границе сети позволяет быстро выявлять аномалии и вредоносные угрозы, такие как DDoS атаки.

**Автоматизация** обеспечивает высокую скорость сигнализации о DDoS атаке, авто-перенаправление трафика на систему очистки при атаке, в том числе авто-Offload FlowSpec фильтров на маршрутизаторы, и соответственно, высокую доступность сети и сервисов.

**Оптимизация** сетевых ресурсов на основе комплексных отчетов о трафике, клиентских и географических данных для более разумного планирования трафика.

**Монетизация** на платформе Arbor SP, которая используется для визуализации сети и обнаружения угроз, позволит легко предоставлять и поддерживать новые услуги, такие как анализ клиентского трафика и облачная очистка от вредоносного трафика.



# Arbor SP 7000/Virtual Appliance

## SP 7000 – Hardware appliance

### Платформа

- 2 x Intel Xeon E5-2648L v3 (12 cores)
- 32GB DDR
- RAID 6x480 SSD
- 2RU, AC/DC

### Производительность:

- до 240 000 Flows Per Second

### Лицензирование:

- **Purchase** бессрочные лицензии Arbor SP Flex, приобретаемые по мере необходимости, далее оплачивается только ежегодное техническое обслуживание и поддержка. Идеально подходит для быстрорастущих ISP, ориентированных на CAPEX-модель.
- **Site License** бессрочные лицензии Arbor SP Flex, охватывающие всю инсталляцию (текущие или прогнозируемые потребности), далее оплачивается только ежегодное техническое обслуживание и поддержка. Идеально подходит для больших, быстрорастущих и CAPEX-ориентированных ISP;
- **Subscription** годовая подписка, которая включает в себя обслуживание и поддержку. Отлично подходит для OPEX-ориентированных организаций, адаптирующихся к быстро меняющимся рыночным условиям.

## SP Virtual Machines

### Платформы:

- VMware vSphere / 8-32 Core, 16-32 GB RAM, 100 GB Storage
- KVM QEMU / 8-32 Core, 16-32 GB RAM, 100 GB Storage
- Xen Cloud Platform / 8-15 Core, 16-32 GB RAM, 100 GB Storage

### Производительность:

- VMware vSphere до 300 000 Flows Per Second
- KVM QEMU до 300 000 Flows Per Second
- Xen Cloud Platform до 120 000 Flows Per Second



# Arbor TMS 2600/2800

## TMS 2600

### Платформа

- 2 x Intel Xeon E5-2608L v3 (6 cores)
- 32GB DDR
- RAID 2x120 SSD
- 2RU, AC/DC

### Лицензируемая производительность:

- 1Gbps, 2Gbps, 5Gbps
- 10Gbps, 15Gbps, 20Gbps

### Сетевые интерфейсы:

- 4, 8 или 12x1GE
- 4 x 10GE, 4 или 8x1GE

## TMS 2800

### Платформа

- 2 x Intel Xeon E5-2648L v3 (12 cores)
- 64GB DDR
- RAID 2x240 SSD
- 2RU, AC/DC

### Лицензируемая производительность:

- 10Gbps, 20Gbps, 30Gbps и 40Gbps

### Сетевые интерфейсы:

- 4 или 8x10GE

# Arbor TMS HD1000/HD1000+

## TMS HD1000

### Платформа

- 2 x Intel Xeon E5-2648L v3 (16 cores)
- 32GB DDR
- RAID 2x480GB SSD
- 2RU, AC/DC

### Лицензируемая производительность:

- 20 - 160 Gbps
- 110 Mpps+

### Сетевые интерфейсы:

- 4x100GE + 8x10GE или 16x10GE интерфейсы

## TMS HD1000+

### Платформа

- 2 x Intel Xeon E5-2648L v3 (16 cores)
- 32GB DDR
- RAID 2x480GB SSD
- 2RU, AC/DC

### Лицензируемая производительность:

- до 400 Gbps
- 220 Mpps+

### Сетевые интерфейсы:

- 4x100GE + 8x10GE или 16x10GE интерфейсы

# Arbor Virtual TMS

## vTMS

### Гипервизор

- VMware vSphere 5.5+
- KVM kernel 3.19 QEMU 2.0

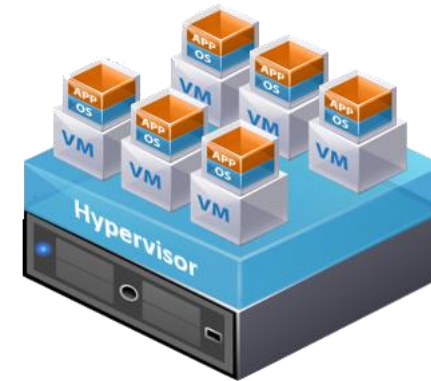
### Аппаратные требования:

- vCPUs: 3-32; NICs: 1 to 10; Memory: 10-53 GB; Storage: 100 GB

### Производительность на Instance:

- Пропускная способность при инспектировании 1-30 Gbps

## Virtual Appliances



Pre-installed  
Pre-configured  
OS & App Stack



Коммерческие вопросы:

Геннадий Соколов

[gsokolov@netwell.ru](mailto:gsokolov@netwell.ru)

+7.985.279.99.38

Алексей Пироженко

[apirozhenko@netwell.ru](mailto:apirozhenko@netwell.ru)

+7.915.098.89.08

Технические вопросы:

Максим Бузмаков

[mbuzmakov@netwell.ru](mailto:mbuzmakov@netwell.ru)

+7.909.664.23.68

