«Системы класса NPMD ViaviSolutions, Межсетевые экраны и ИТ безопасность компании Clavister»

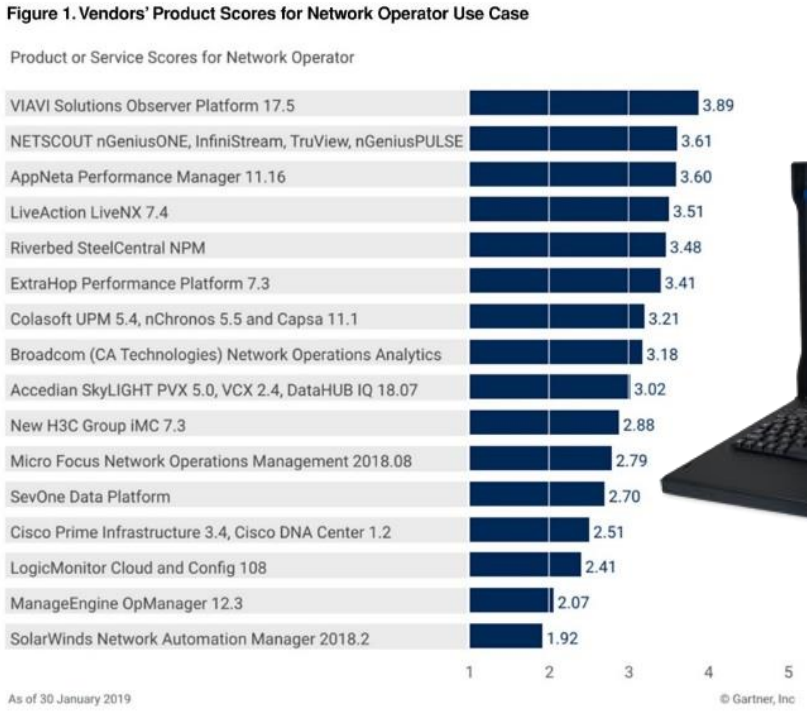
- Ярослав Баранов, TCM B&H
- Андрей Поцелуев, ТОО «Линкмастер»

TCM B&H ТОО «Линкмастер»

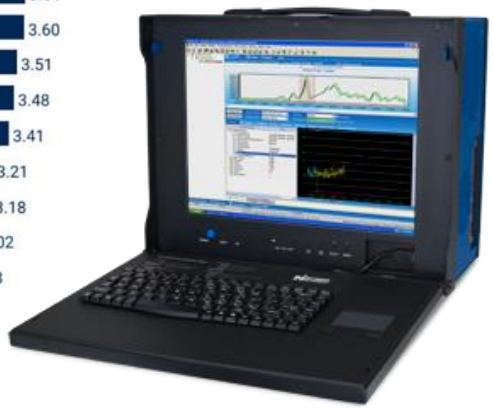
- TCM основана в 1994 г. в Вене, Австрия
- Дистрибюция продукции для телекоммуникаций и энергетики
- Работает на рынке РФ и СНГ с 1996г.
- Является эксклюзивным дистрибютором по оборудованию синхронизации Microsemi (бывш. Symmetricom), систем класса NPMD ViaviSolutions, Firewalls Clavister, Signalling Firewalls Cellusys
- Партнер по Казахстану – ТОО «Линкмастер», www.linkmaster.kz

Система Viavi класса NPMD: Apex-Observer-Gigastor

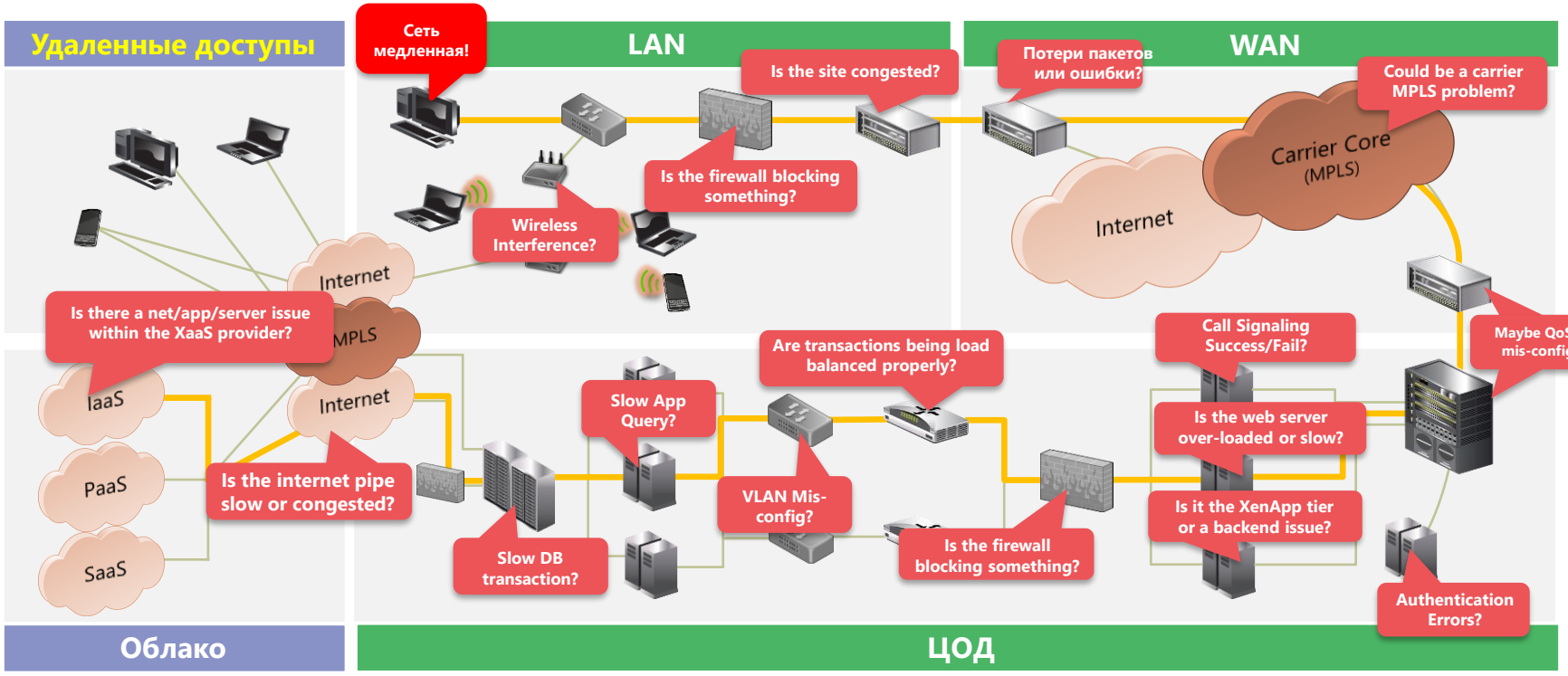
- Apex-Observer-Gigastor полнофункциональная NPMD система пассивного мониторинга трафика анализаторами Gigastor от портативного лаптопа до стоечных серверов для записи трафика и транзакций до нескольких месяцев



Source: Gartner (February 2019)



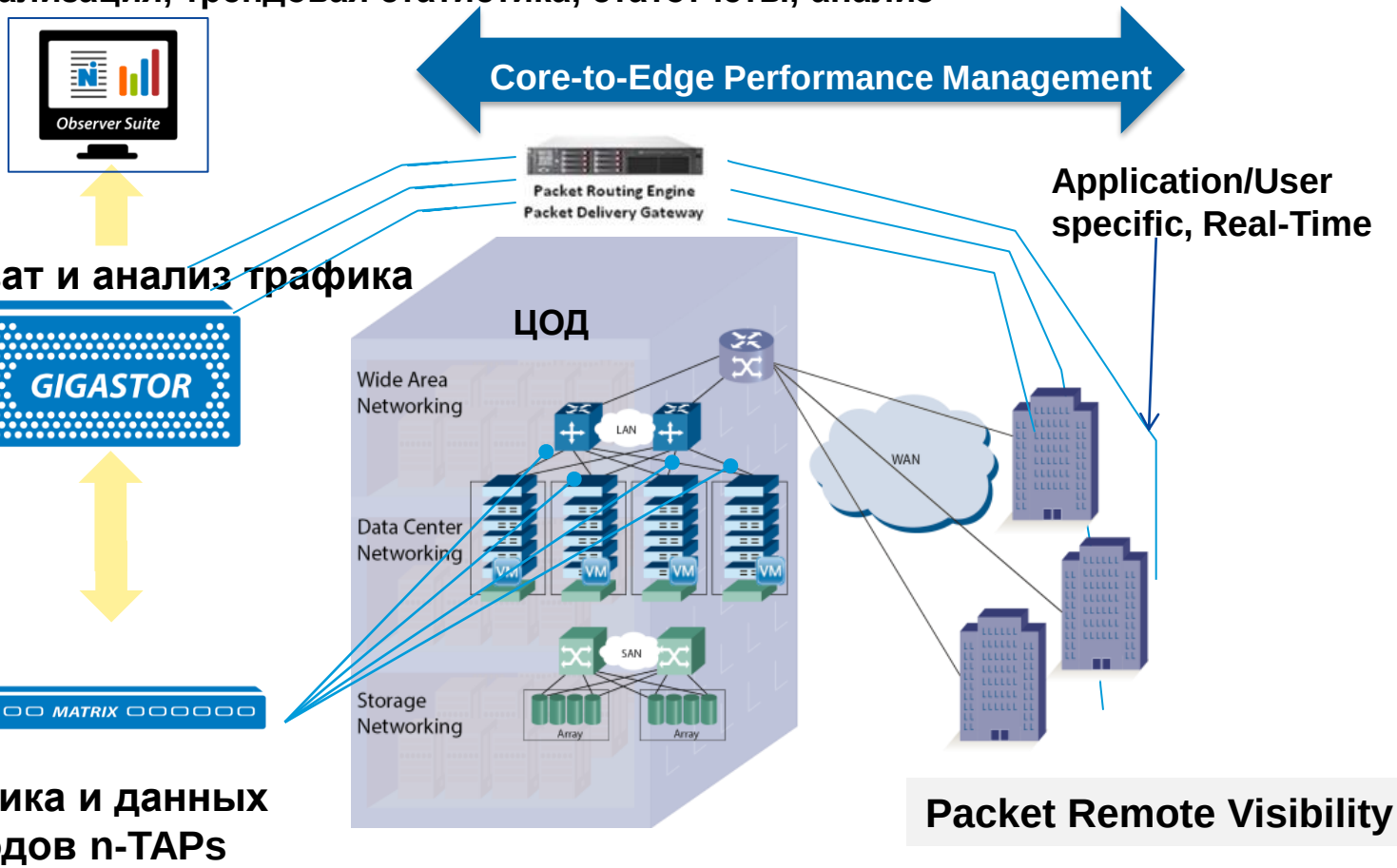
Общий кейс: где искать проблему в сети: WAN или локальная сеть или приложение или сервер или ПК или канал связи!



Главный KPI – QoE и локализация и диагностика проблемы!

Network and Application Performance Management Solution

Observer - Визуализация, трендовая статистика, статотчеты, анализ



Аггрегация трафика и данных
С помощью отводов n-TAPs

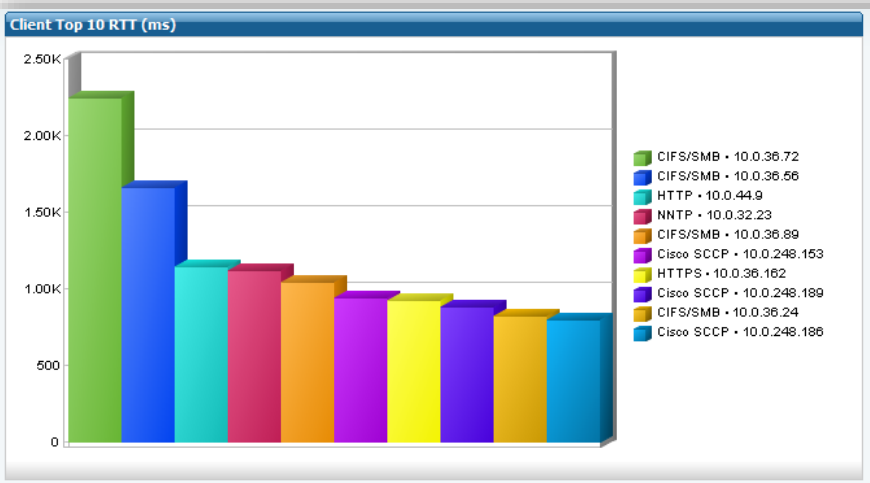
Packet Remote Visibility

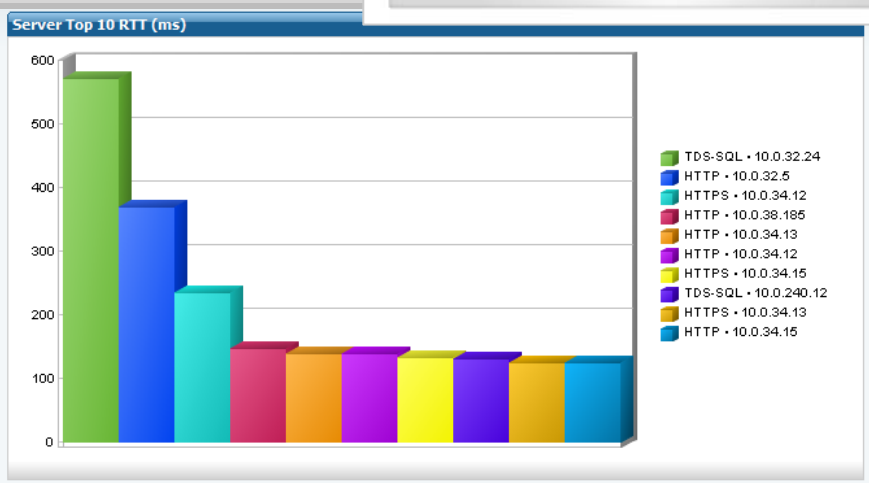
Дополнение к существующей Network Management Solution – типовая таблица функционала

	Текущая Network Management System	VIAVI Network Performance Management System Apex-Observer-Gigastor
Мониторинг оборудования, состояние и диагностика (SNMP, WMI и др.)	Yes	No
Оценка удовлетворенности конечного пользователя QoE	No	Yes
Углубленная диагностика причины проблем производительности и безопасности	No	Yes
Углубленный аналих пакетов методами DPI	No	Yes
Много-узловой анализ транзакций медленных линков с потерями пакетов, высокими задержками и джиттером	No	Yes
Диагностика и мониторинг качества услуг VOIP и VideoConferencing	No	Yes

Observer Reporting Server (ORS) – сервер статотчетности

- Углубление до причины и разрешения проблемы
  - Summary application awareness
  - Межсегментная и межсетевая диагностика

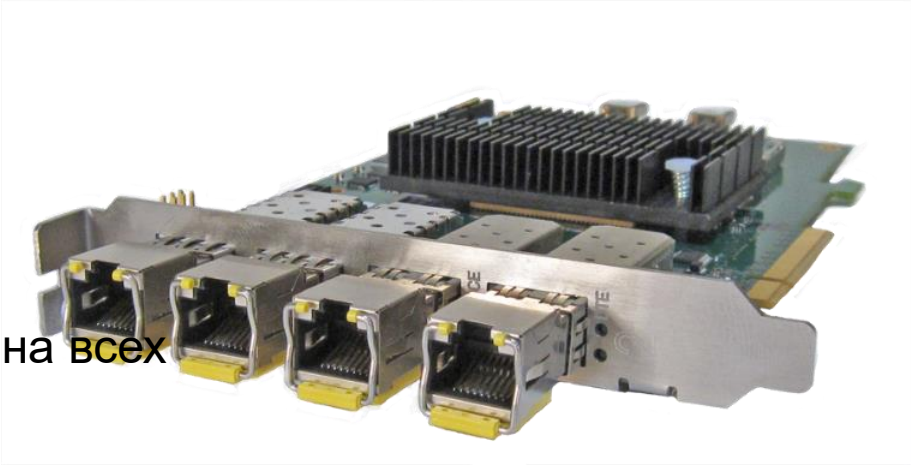




Top 10 Client / Server TCP RTT (ms)

Drill Down	Application Name	Client IP Address	Response Time		Server IP Address	Response Time			Observed		Bytes			Probe	
			Client Average (ms)	Client Average (ms)		Server Average (ms)	Server Average (ms)	Server Maximum (ms)	Connections	Connections	Client	Server	Total	IP Address	Instance
	CIFS/SMB	10.0.36.72	4034.115	2485.240	10.0.32.14	0.742	0.535	90.754	159	221	10.6M	132M	143M	10.0.32.20	Core-Partial Capure
	CIFS/SMB	10.0.36.56	3030.977	2399.281	10.0.32.14	0.369	0.455	43.839	185	255	7.96M	134M	142M	10.0.32.20	Core-Partial Capure
	CIFS/SMB	10.0.36.89	2396.189	2241.136	10.0.32.14	3.208	0.500	88.799	148	229	6.04M	90.4M	96.5M	10.0.32.20	Core-Partial Capure
	HTTP	10.0.36.53	1827.333	1690.757	10.0.34.12	343.013	342.140	372.829	13	35	22.2K	210K	233K	10.0.32.20	Core-Partial Capure
	CIFS/SMB	10.0.36.24	1645.527	1698.047	10.0.32.14	0.561	0.257	29.930	130	164	18.0M	182M	200M	10.0.32.20	Core-Partial Capure
	HTTPS	10.0.36.55	1386.842	614.568	10.0.34.15	243.768	221.993	322.480	10	17	27.6K	152K	180K	10.0.32.20	Core-Partial Capure
	NetBIOS session	10.0.36.48	1340.646	2306.230	10.0.32.14	3.712	10.473	81.306	37	196	8.23M	57.4M	65.6M	10.0.32.20	Core-Partial Capure
	HTTP	10.0.44.9	1146.682	---	10.0.32.14	1.162	---	1.162	1	---	1.12K	912	2.03K	10.0.32.20	Core-Partial Capure
	NNTP	10.0.32.23	1124.007	---	10.0.40.55	36.122	---	36.122	1	---	256	413	669	10.0.32.20	Core-Partial Capure
	Cisco SCCP	10.0.248.153	941.898	---	10.0.240.10	0.203	0.182	7.439	525	351	281K	147K	429K	10.0.32.20	Core-Partial Capure

Карты захвата трафика Gigastor Gen2



- Собственная разработка Виави
  - 1 Gb, 10 Gb**, 40 Gb, 100Gb**
- Ключевые свойства
  - Обработка в реальном времени на всех линейных скоростях
  - Full-duplex, line-rate capture
  - Streams directly to physical system memory
- Гибкость конфигурирования
  - До 12x1G или 10G портов на карту
  - SFP+: медь или оптика

Gen2 Delivers
✓ Performance
✓ Flexibility
✓ Adaptability

- Адаптация под систему
  - Устранение дублирования пакетов, фильтрация, анализ
  - Аппаратная обработка для высоких скоростей
  - Апгрейд флеш-память

Семейство анализаторов трафика GigaStor

Все анализаторы GIGASTOR используют Gen2™ карты захвата до 100G

Rack Size: 2U
Storage: 4 TB - 16 TB

Rack Size: 5U
Storage: 16 TB - 48 TB

GigaStor Upgradeable

- Data center/ branch facilities/ network edge
- Field upgradeable without rack removal
- 4 to 48 TB capacity
- 1, 10, 100 Gb

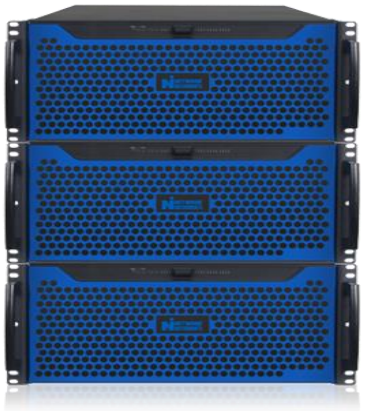
GigaStor Portable

- Transportable design
- 4 or 8 TB capacity
- **1, 10, 40 Gb**

Rack Size: 5U+
Storage: 48 TB+

GigaStor Expandable

- Data center/large branch
- Field expandable
- 48 TB to 1 PB capacity
- **1,10, 40, 100 Gb**

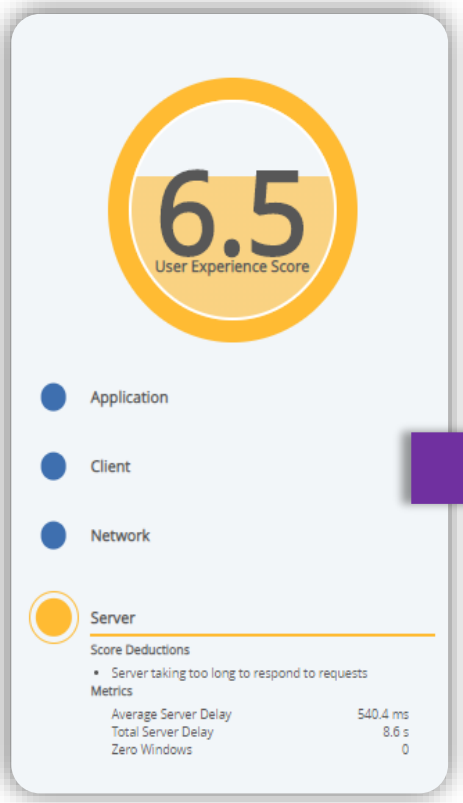


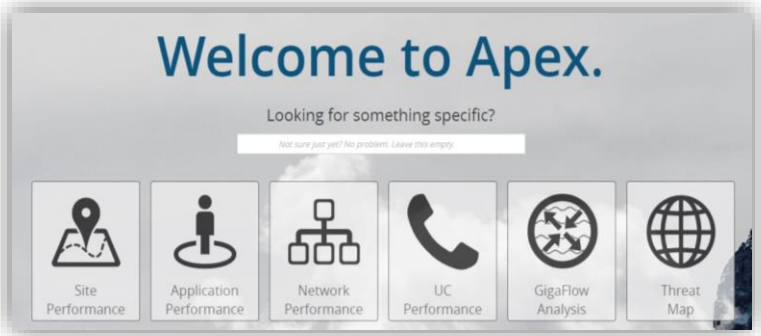
Rack Size: 5U+
Storage: 144 TB+

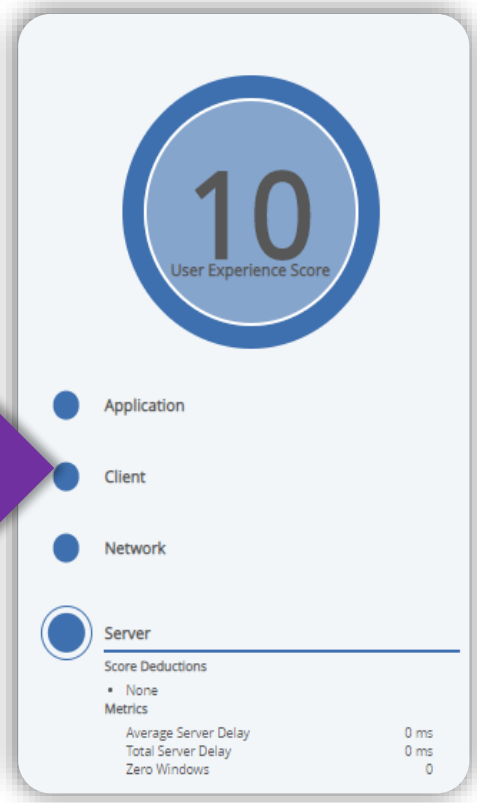
GigaStor 100 Gb Wire Speed

- Large data center/ enterprise core
- World's fastest 10 Gb write-to-disk appliance
- 144 or 288 TB capacity
- **10, 40, 100 Gb line rate**

VIAVI Apex-Observer-Gigastor : EUE Score Difference







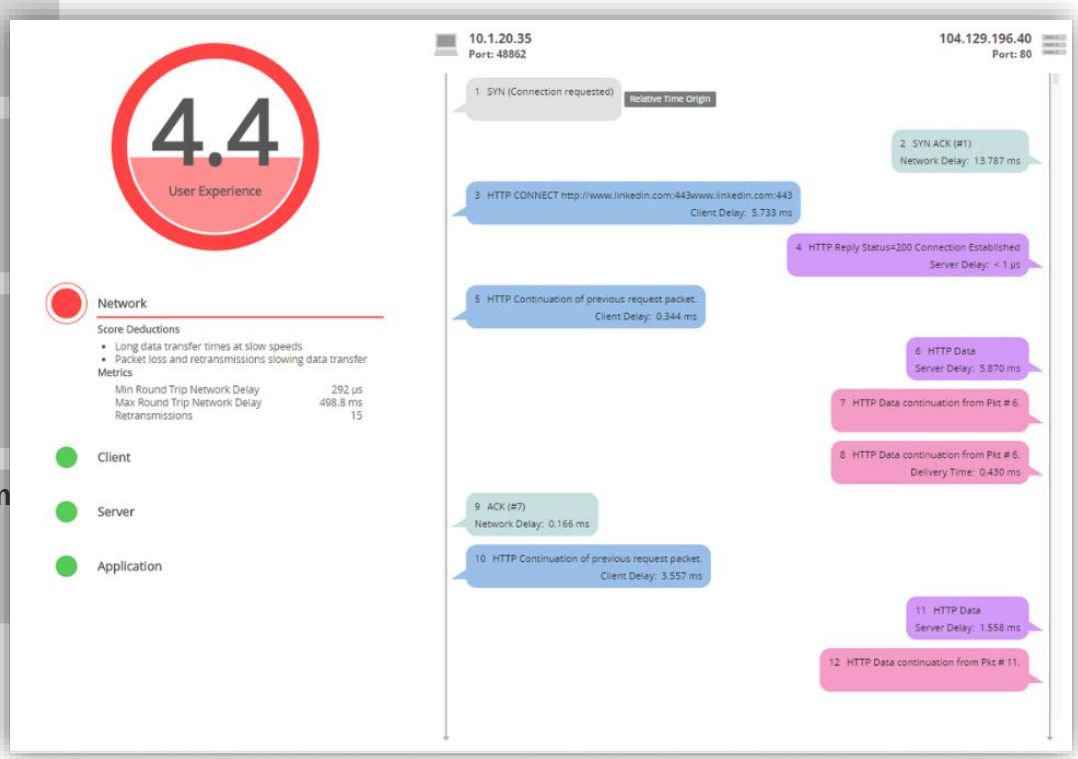
Apex-Observer-Gigastor : категории деградации EUE

Network
- Internal Congestion
- Slow Processing

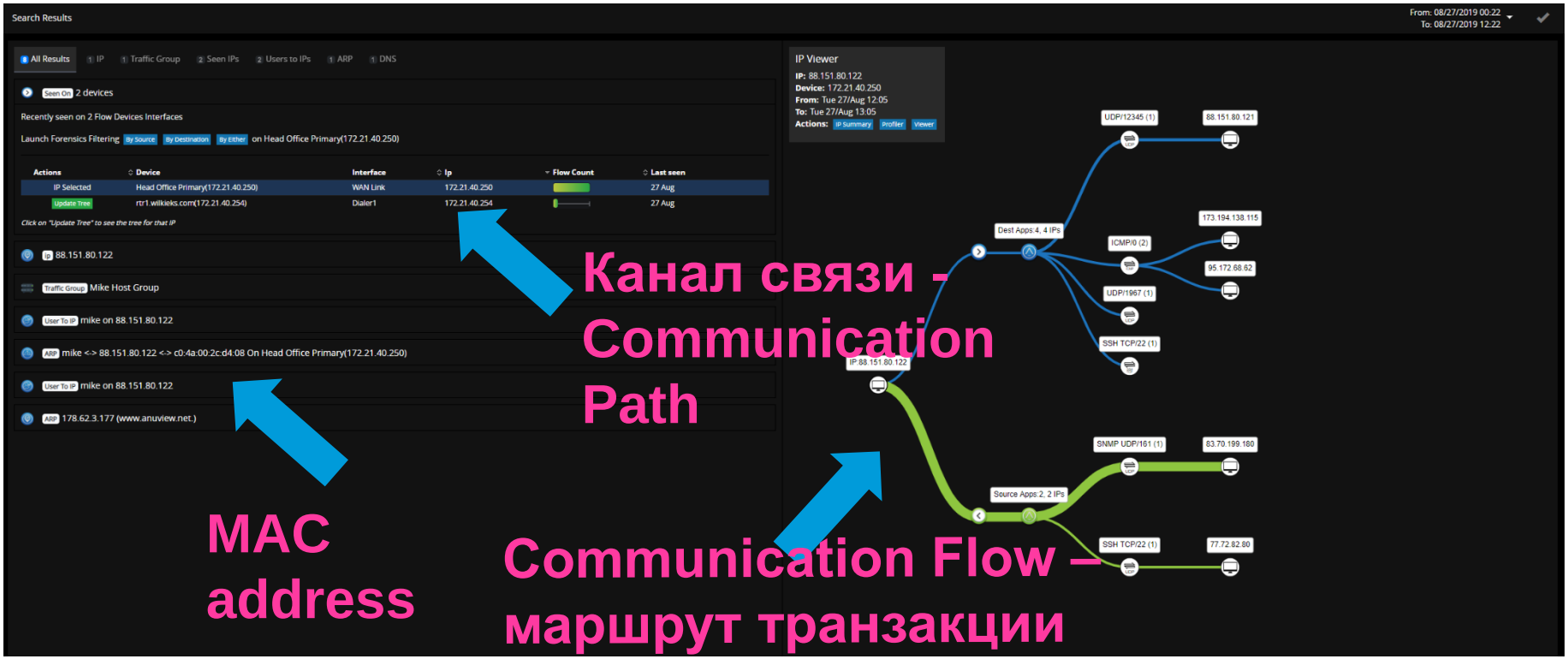
Client
- Congestion
- Low Bandwidth
- Lost Packets
- Latency

Server
- Internal Congestion
- Slow Processing

Application
- Long Processing Tim
- Long Transfer Time
- Inefficient Use of Network Resources

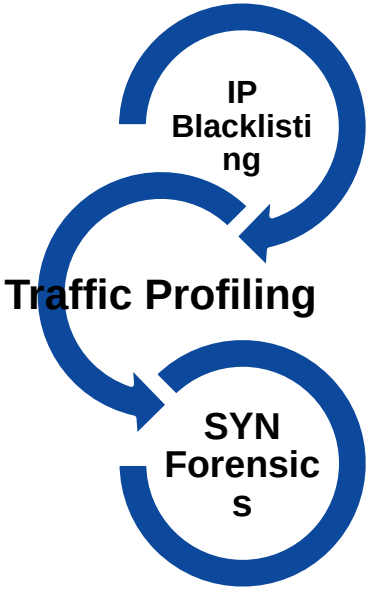


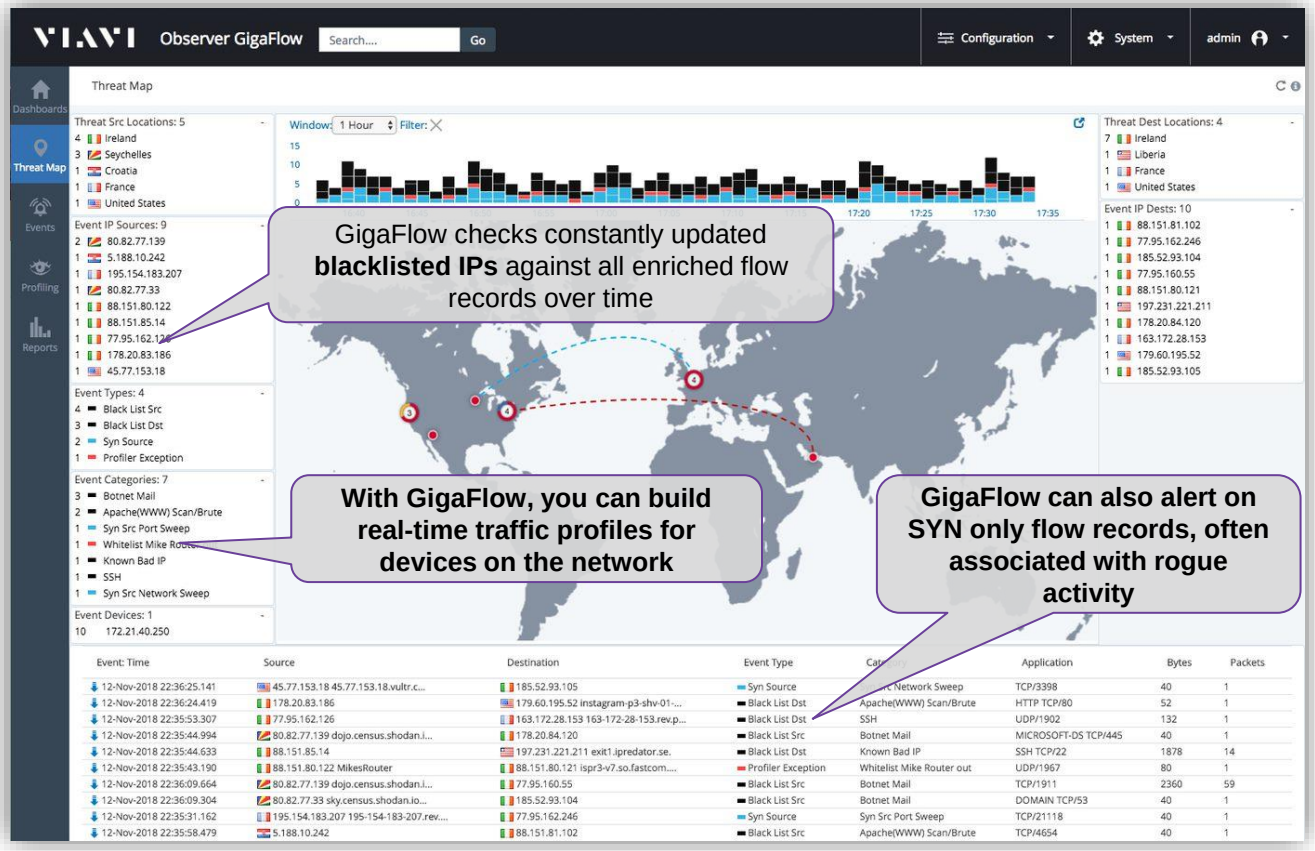
Пример экрана GigaFlow: Кто подключен к сети, кто проводит транзакции? Маршруты транзакций в сети?



Интегрированная карта угроз

Observer GigaFlow агрегатирует три категории угроз на карту реального времени:

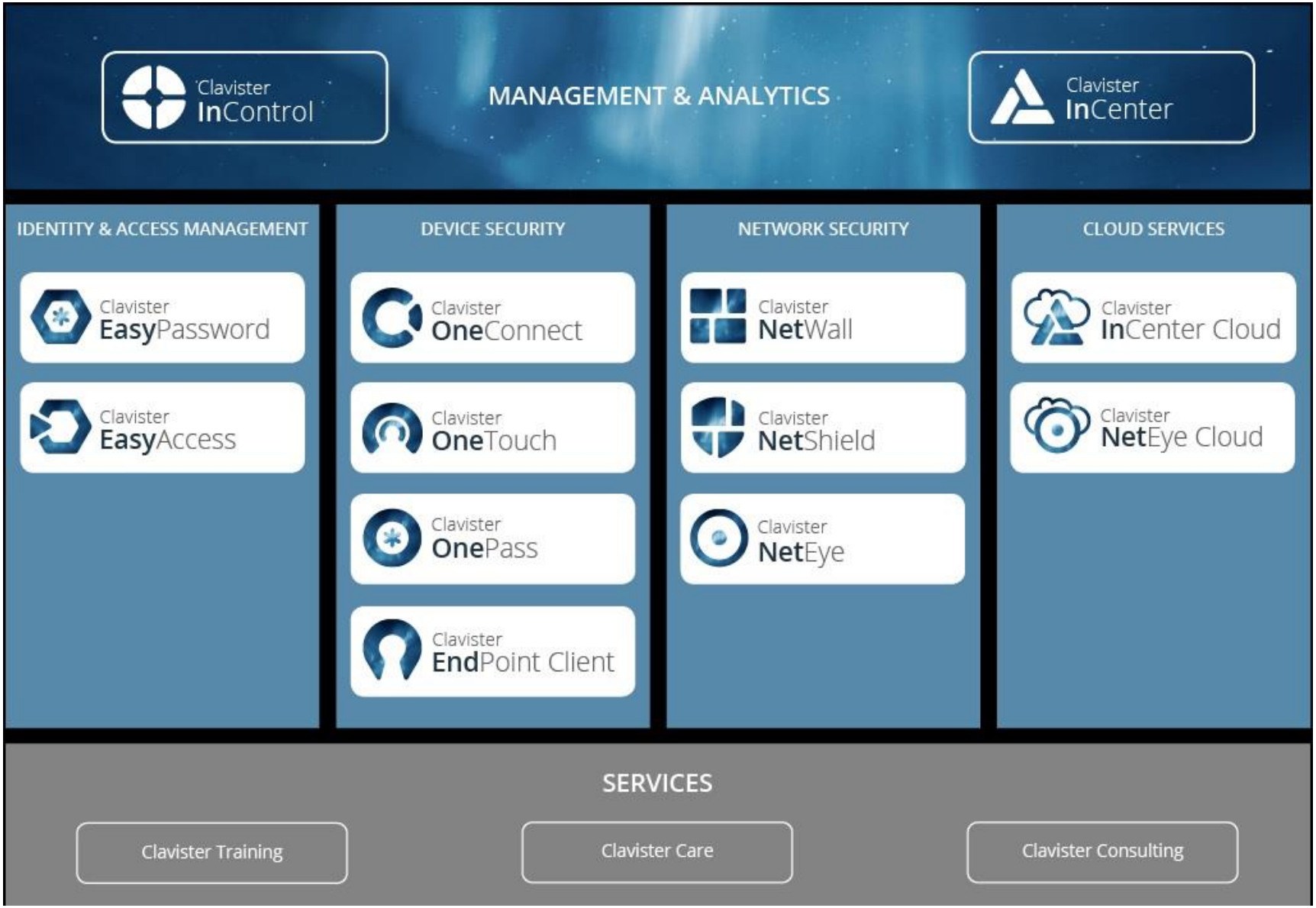




Clavister

Продукты безопасности для Телеком операторов и корпоративного сектора
Product and Solution Overview

Структура продуктов ИТ безопасности Клавистер



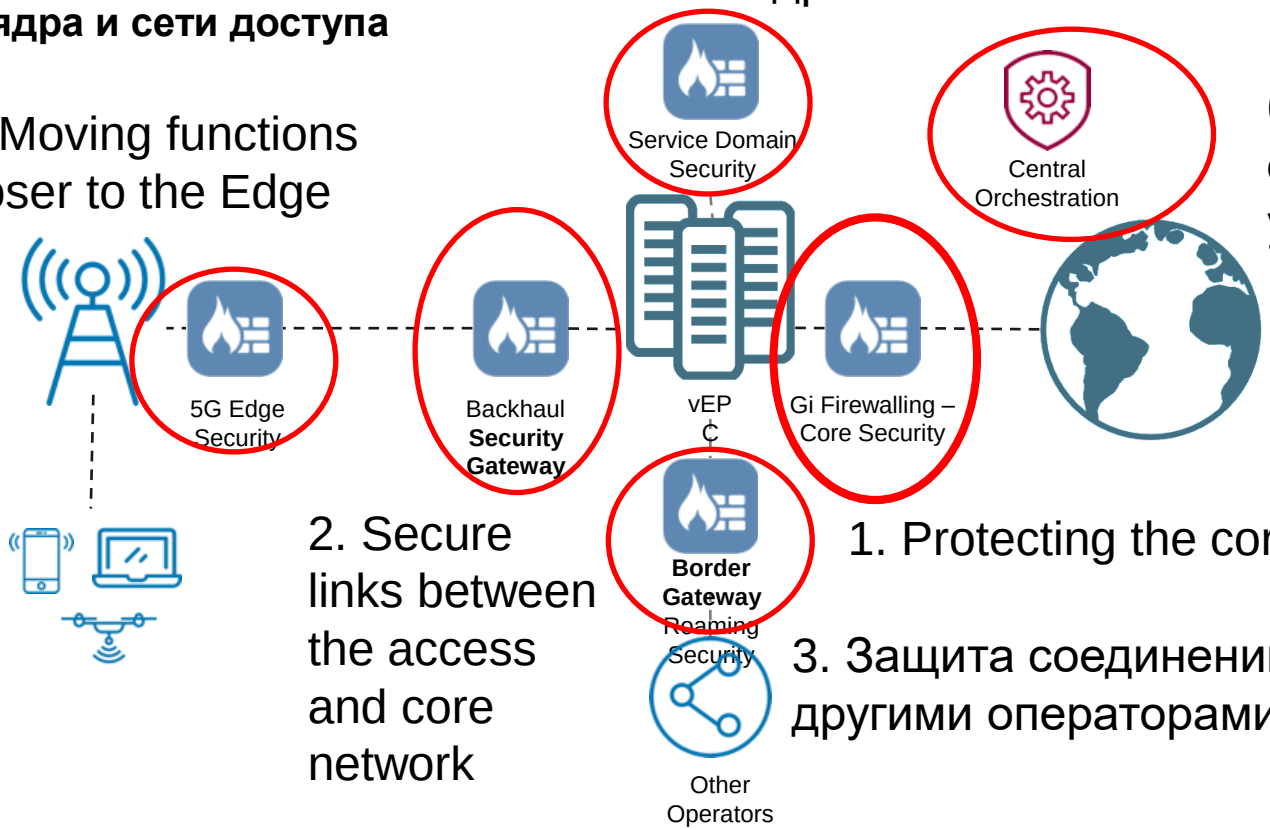
Виртуальные решения безопасности сетей связи

clavister

4. Защита критичных бизнес систем Ядра сети

Защита ядра и сети доступа

5. Moving functions closer to the Edge



6.Централизованное управление

2. Secure links between the access and core network

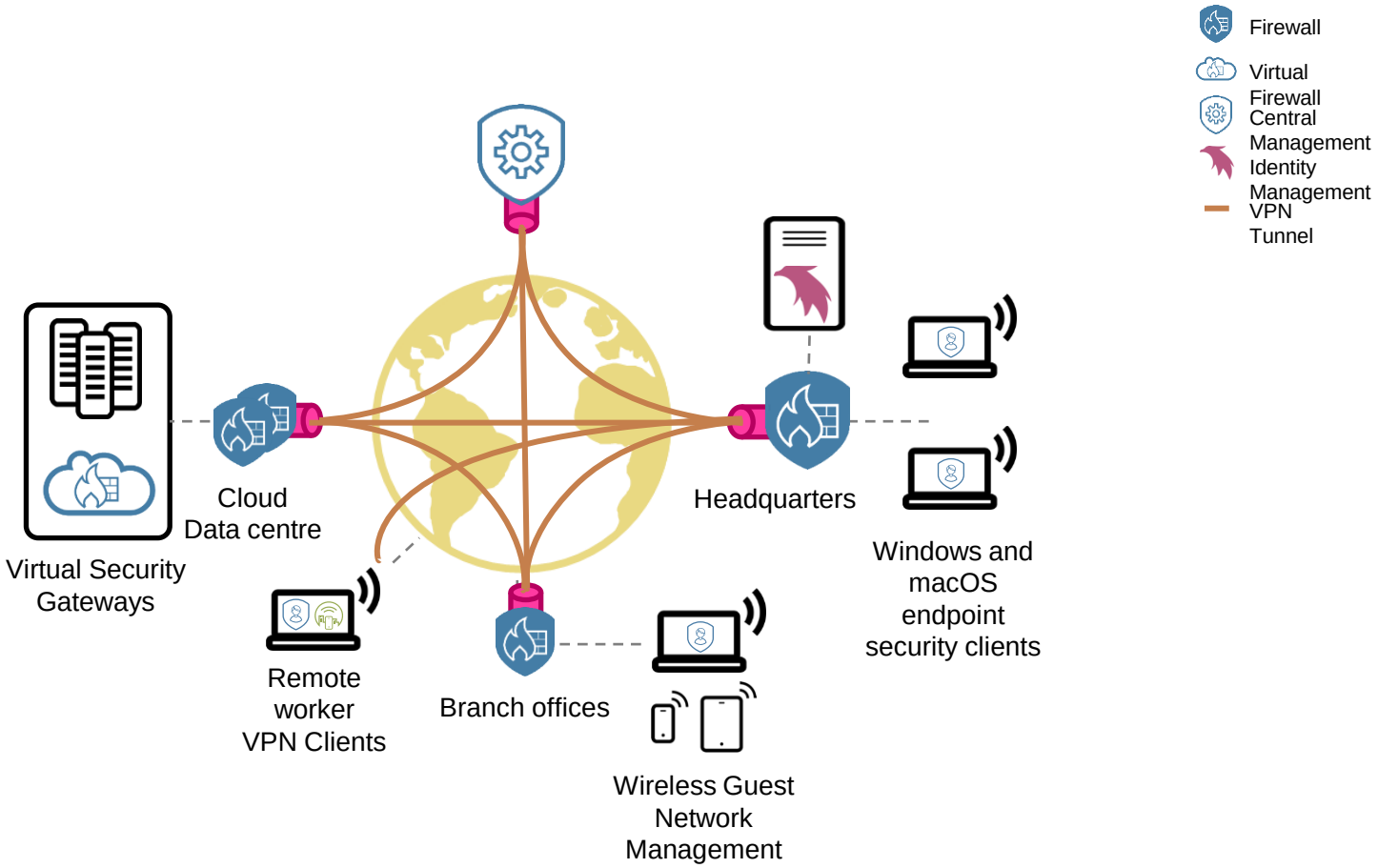
1. Protecting the core network

3. Защита соединений с другими операторами

SECURITY BY SWEDEN

Защита телеком сигнализации: GTP, SIP, CMPv2, CG-NAT, DNS ALG, SCTP, High Availability

Комплексная защита корпоративных сетей

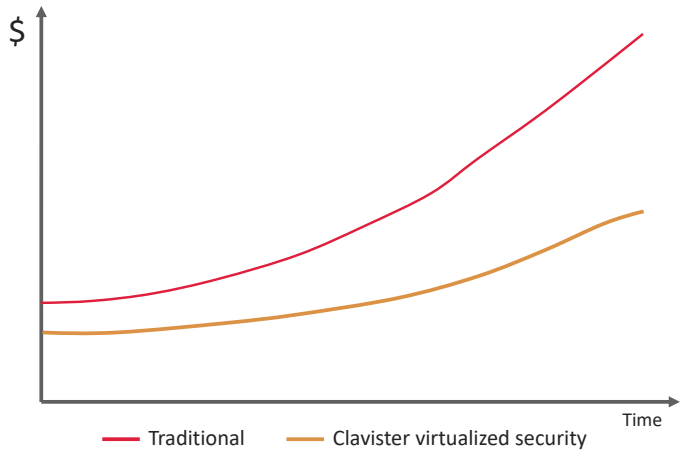


Бизнес модель под клиента

Максимизация преимуществ NFV / SDN

Оплата за аггрегатную емкость

Получить безлимитное кол-во VNFs



Гибкая модель запуска и лицензирования с целью уменьшить ТСО заказчика – Управление из единого центрального решения с индустриальными стандартами

Clavister – эко система и партнеры

Интеграция в продукты Clavister Firewall эко системы лучших мировых продуктов в качестве компонент для кейсов заказчиков:

McAfee

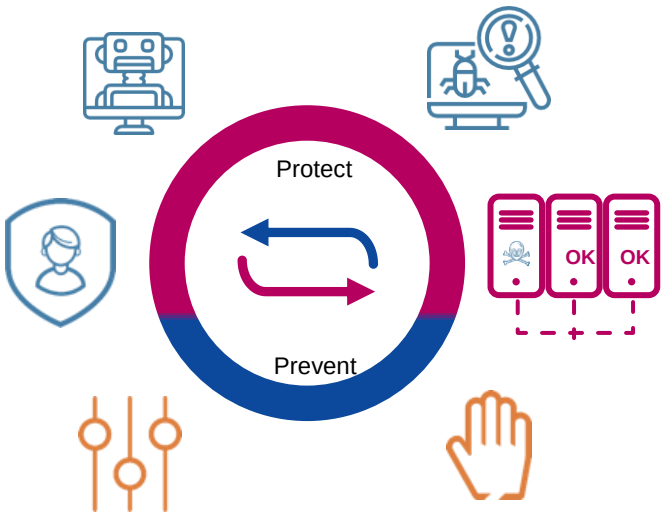
Providing malware signature profiles for Intrusion Prevention System

Bitdefender

Providing industry's best performing Endpoint protection

ENEA Qosmos Division

Enabling Application Control with Deep Packet Inspection



MAXMIND

Providing GeoIP® database for accurate geofencing

KASPERSKY lab

Providing antimalware signatures, definitions for screening

WEBROOT

Empowering IP Reputation Feeds

ContentKeeper

Providing URL databases for Web Content Filtering

Платформы & Совместимость

Virtualisation

openstack. KVM vmware vSphere Hyper-V

Cloud

Google Cloud Microsoft Azure aws

Appliances

Аппаратные платформы

Clavister E10
Dektop

Clavister E20
Dektop

Clavister E80
Dektop

Clavister W20
19”, 1U Rack-mounted

Clavister W30
19”, 1U Rack-mounted

Clavister W40
19”, 1U Rack-mounted

Clavister W50
19”, 1U Rack-mounted

Clavister NET80
Interface module

Clavister NET81
Interface module

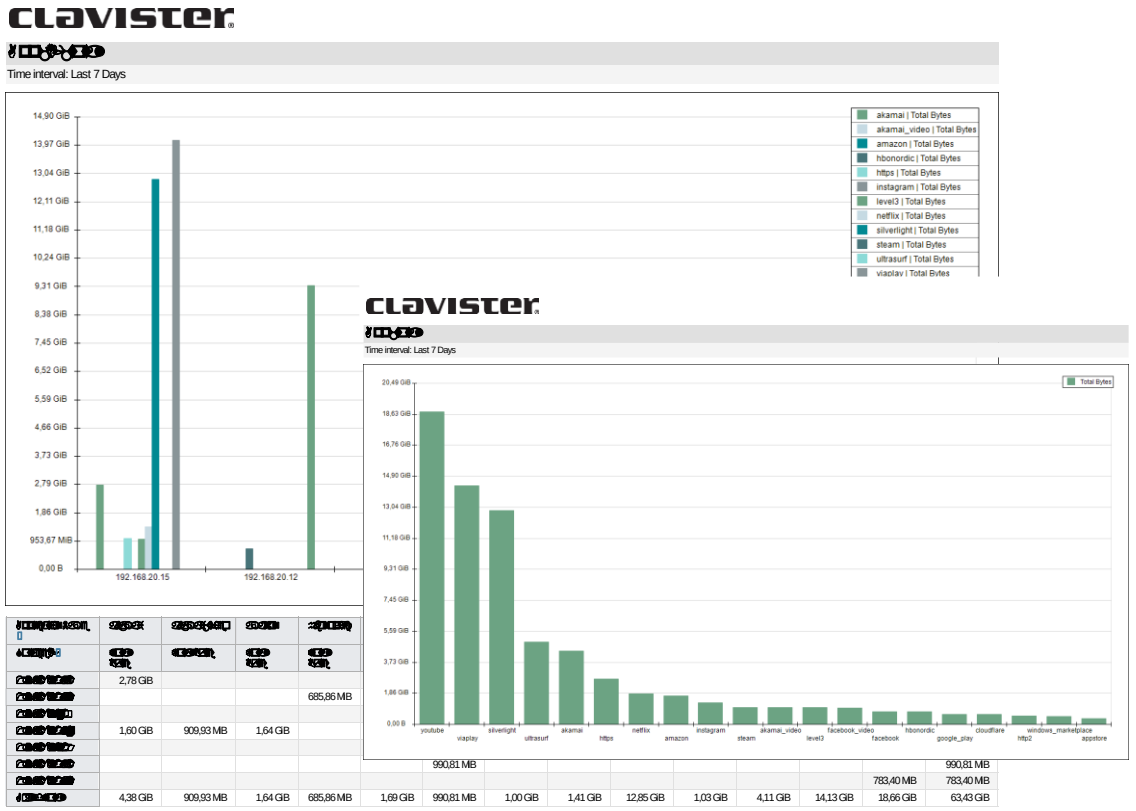
Clavister NET120
Interface module

Clavister NET140
Interface module

SECURITY BY SWEDEN

Статотчетность

- Detailed reporting per user per services
- Traffic volume and connection attempts
- Identifying users via Active Directory integration



	2,78 GiB												
				685,86 MiB									
	1,60 GiB	909,93 MiB	1,64 GiB										
						990,81 MiB						990,81 MiB	
											783,40 MiB	783,40 MiB	
	4,38 GiB	909,93 MiB	1,64 GiB	685,86 MiB	1,69 GiB	990,81 MiB	1,00 GiB	1,41 GiB	12,85 GiB	1,03 GiB	4,11 GiB	14,13 GiB	18,66 GiB	63,43 GiB

EasyAccess

Multi-factor Authentication

Single Sign-On

Clavister
EasyAccess

Multi-Factor Authentication (MFA)

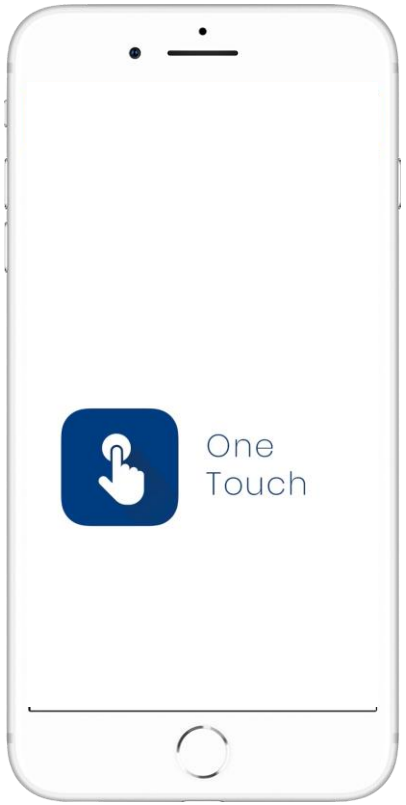
Something you KNOW

Something you HAVE

Something you ARE

Clavister
OneTouch

- Простой 2-шаговый портал входа
- Smooth user experience: push notification
- Approve authentication / signing request
- Защитный ключ с Pin Code или отпечатком пальца* или лица*



Available on the App Store

ANDROID APP ON Google play

*for supported devices

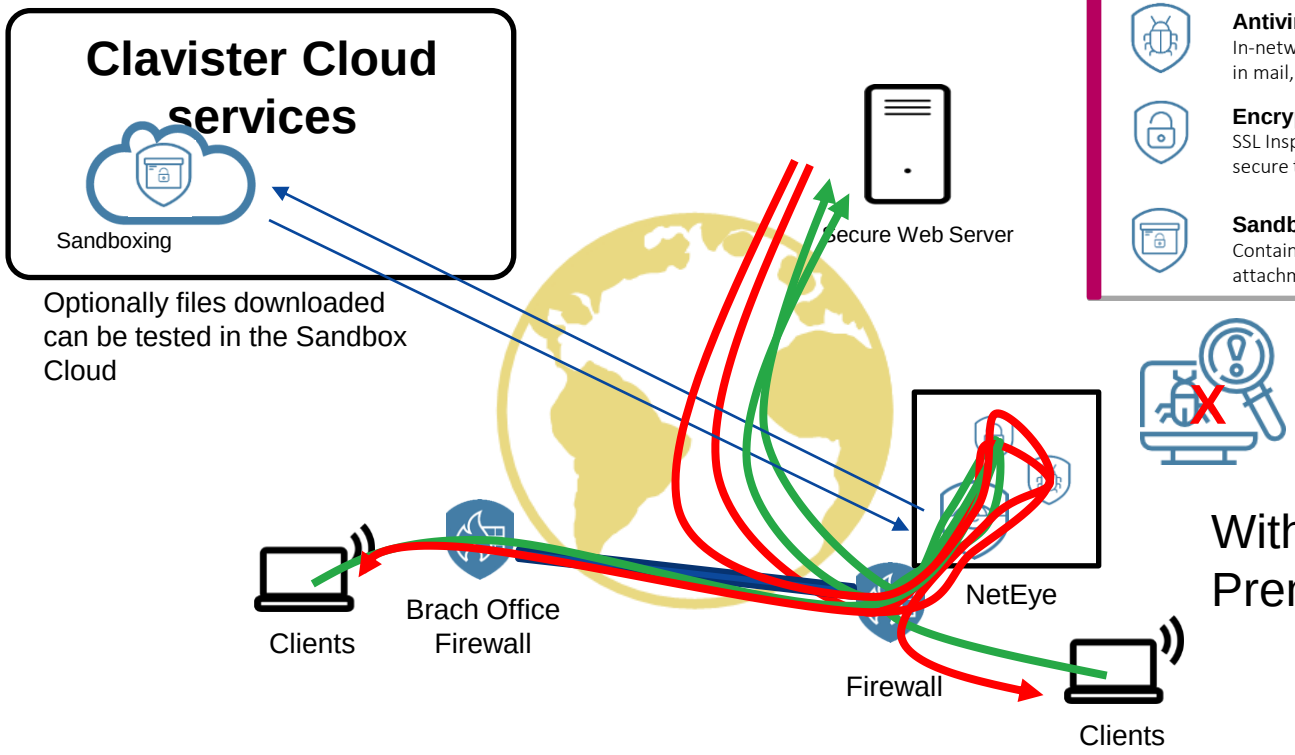
Инспектирование и нейтрализация угроз встроенных в SSL

Clavister NetEye

- Улучшение защиты от продвинутых угроз – для дополнения Clavister или любого другого Firewall
- До 3,5 G производительность, емкость инспектирования 2 Gbps SSL (3500 юзеров)
- До 3 движков сканирования вирусов
- **Улучшение существующей инфраструктуры безопасности**

Clavister NetEye Appliance

Advanced Threat Protection



Protect

Antivirus/Malware Scanning
In-network antivirus scanning of attachments in mail, web and file downloads

Encrypted Traffic Inspection
SSL Inspection to look inside untrusted secure traffic

Sandboxing
Contained detonation of suspected attachments and downloads

★ ANIMATED

Спасибо!