



Infosim® StableNet®

General Introduction

Automated Network & Service Management



1&1 VERSATEL

BMW

LIDL + SCHWARZ IT GROUP

STATE STREET

STANFORD
UNIVERSITY

CITY OF LOS ANGELES
LOS ANGELES UNIFIED
SCHOOL DISTRICT (LAUSD)

VODAFONE UK

MTN NIGERIA


NEOM CITY PROJECT




- **Founded 2003 as a privately held company**
- **Target market for StableNet®**
 - Large networks / IT installations at network operators, companies, public authorities and utilities
 - Medium and small networks / installations at SMEs or similar with StableNet® as a Service
- **Corporate Strategy**
 - Software development and maintenance 100% in house
 - Worldwide sales via Würzburg, the sales locations Austin (Texas, USA) and Singapore, and through partners
 - Above 100 employees with strong growth planned during the next years


StableNet and it's 3 Key Benefits



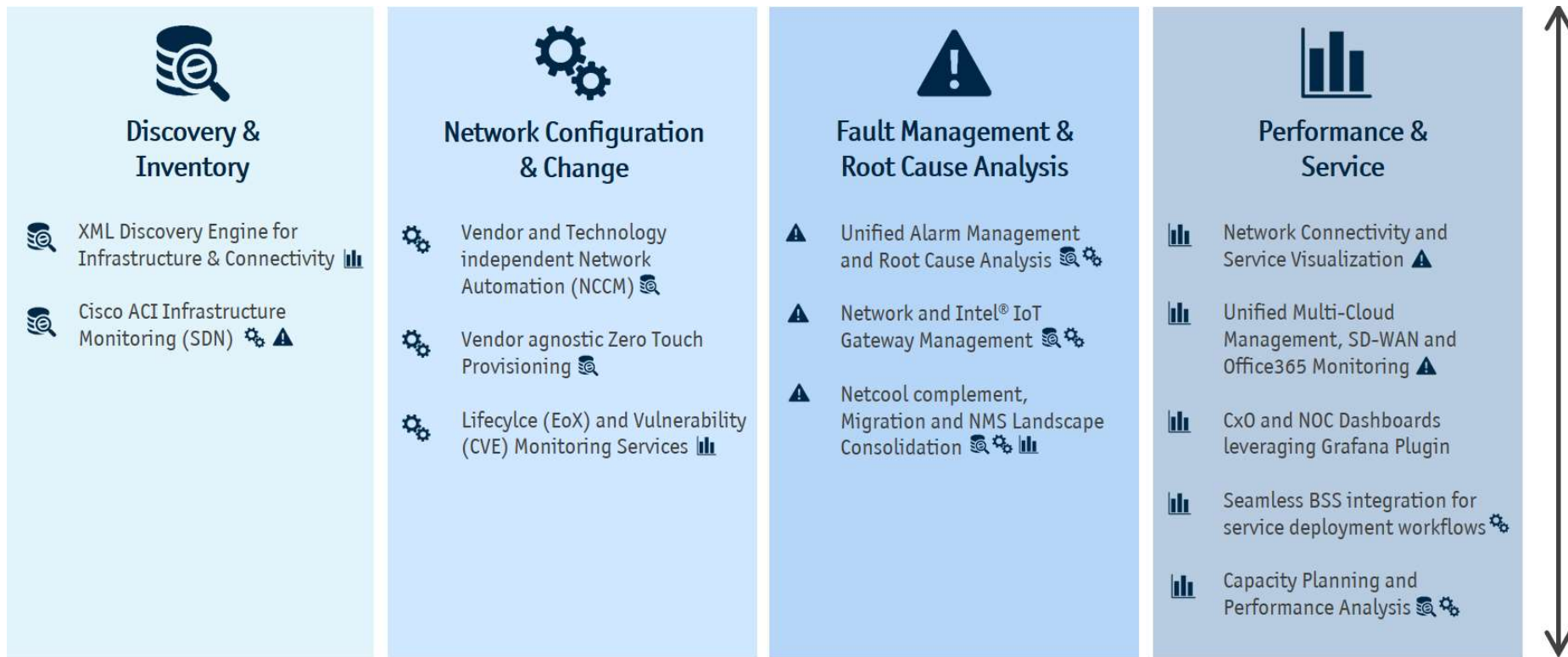
 **Automation:** reduces time spent on repetitive tasks which, along with the consolidation of functionalities, leads to a significant decrease in costs (OPEX and CAPEX).

 **Consolidation:** provides an effective, easy-to-use platform for discovery & inventory, fault, performance, and configuration management within one unified data structure.

 **Scalability:** delivers a flexible framework that is scalable to any sized network.

 **Customization:** enables high levels of flexibility and integration with a large variety of 3rd party systems (both on the South- and Northbound interfaces).

4 Pillars of StableNet



Horizontal Use Case Integration (C³ = cross silos, cross technologies, cross vendors)

TELCO NETWORKS MONITORING & PROVISIONING



- ▶ Broadband Access Networks
- ▶ LoRa Access Networks
- ▶ Mobile Networks (3G/UMTS, LTE/4G, 5G ...)
- ▶ Radio Networks (Point-to-Point)
- ▶ Optical/SDH, Ethernet, IP/MPLS Aggregation
- ▶ Optical, IP/MPLS Backbones
- ▶ Security/Firewalls
- ▶ Voice/Soft switch

IT INFRASTRUCTURE MANAGEMENT



- ▶ Monitoring and Performance Management
- ▶ Alarm Management and “Root Cause” analysis
- ▶ Service and Lifecycle Management
- ▶ Inventory Management
- ▶ Service Provisioning
- ▶ Backup, Restore and Vulnerability Management
- ▶ Analytics and Reporting
- ▶ Consolidation of Management Tools

ENTERPRISE NETS IOT APPLICATIONS



- ▶ Retailers (supervision of cash register systems, video cameras, freeze systems, access systems, facility management)
- ▶ Car Park Operators (utilization, allocation)
- ▶ Facility Management Companies (access systems, video cameras, facility technology)
- ▶ Utility Companies (smart metering, smart grid)
- ▶ Enterprises Industry 4.0 applications (Monitoring and Alarm Management)
- ▶ Transport Companies (railway, bus and all public transportation)
- ▶ Inventory Management
- ▶ Police/Security (e.g. BodyCam)

DATA CENTERS



- ▶ Visualization, monitoring and alarm management of virtualized systems
- ▶ SDN/NFV support
- ▶ Automation and capacity monitoring
- ▶ Service and lifecycle management
- ▶ Inventory management
- ▶ Backup, restore and vulnerability management of network components
- ▶ Analytics and reporting
- ▶ Visualization of VXLAN

Deep Packet Inspection (DPI) is a technology that enables the network owner to analyze internet traffic, through the network, in real-time and to differentiate them according to their payload.

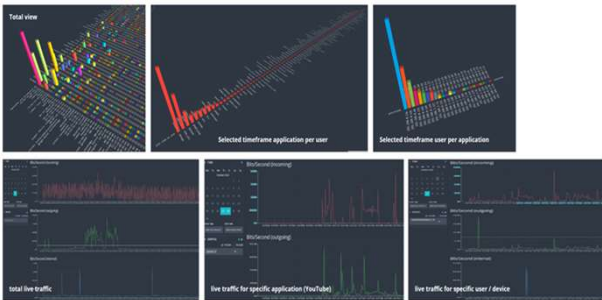
DPI is often used for understanding the performance or behavior of users, which applications they use, how often etc. This helps enterprises to focus on improving service for the important applications. For instance, DPI can indicate the presence of unwanted traffic (bitcoin mining, TOR, ftp, etc) or the health of enterprise critical applications (SAP, Salesforce, Microsoft 365)

DPI analytics in a Network Packet Broker

Advanced DPI analytics running on Cubro appliance. Provide all kinds of measures.

- Performance per Application in select time frame
- Total volume per application in select time frame
- Volume user vs. Application in select time frame
- Total Volume per user in select time frame
- Export to Excel
- Geotrafic analytics
- Threat detection

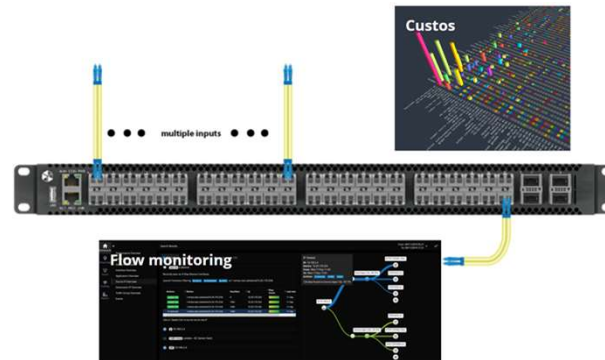
and others



DPI metadata extraction

Metadata extraction based on the Cubro DPI engine, IPFIX / IPFIX & DPI / Cubro CDR.

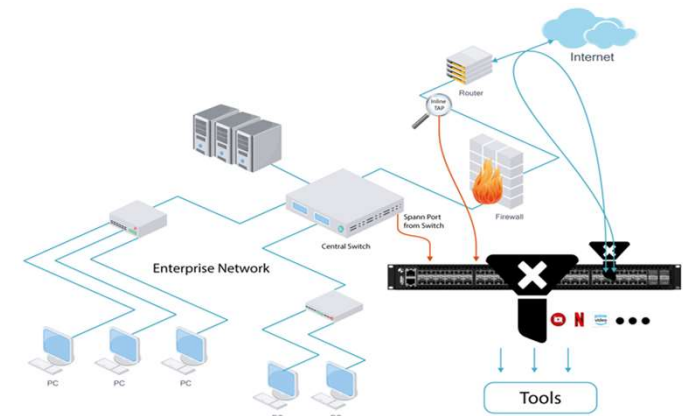
Cubro offers solutions from 100 Mbit/s up to multiple TBit/s input traffic.



Application blocking

Inline Application blocking from Gbit/s to TBit/s traffic. The solution also works based on the Cubro DPI.

This enables the application to block any application like Netflix, YouTube, WhatsApp, TikTok.



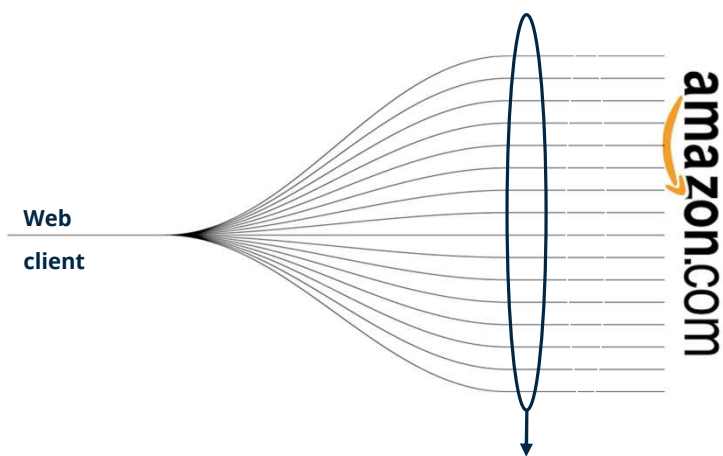
DPI vs Flow Data

Deep packet inspection (DPI) and IP flow monitoring are frequently used network monitoring approaches. Although DPI provides application visibility, detailed examination of every packet is computationally intensive. IP flow monitoring achieves high performance by processing only packet headers, however, it fundamentally provides less detail about the traffic itself.

Application-aware flow monitoring is proposed to combine DPI accuracy and IP flow monitoring performance.



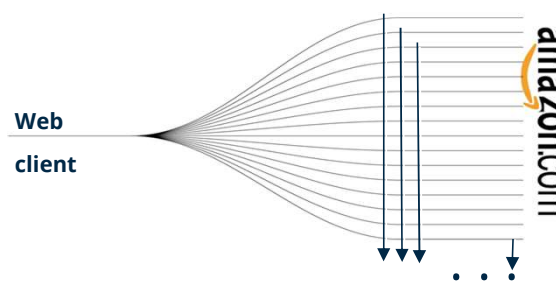
Time window based



For each client, there is a bucket for each application, if needed, and we collect/count all packets for a certain time window (configurable). When the window is closed, an XDR is produced/enriched and sent out. The advantage is, the traffic is reduced on most far point to avoid constraints on the workflow along to the DB.

vs

Flow based



For each 5 tuple connection, one flow is produced; a lot of these flows cannot be detected as Amazon related because the external domain cannot be resolved.

After producing the flow, it is forwarded to the Flow Cache. A Flow Cache can contain hundreds of thousands of entries, and in some cases, into the Millions of entries. (*this costs memory resources*)

When the flows expire, they're exported off to the NetFlow Collector, which will constantly analyse and archive the flows for future reference.

Cubro MetaData vs Flow Data: Huge difference in Volume

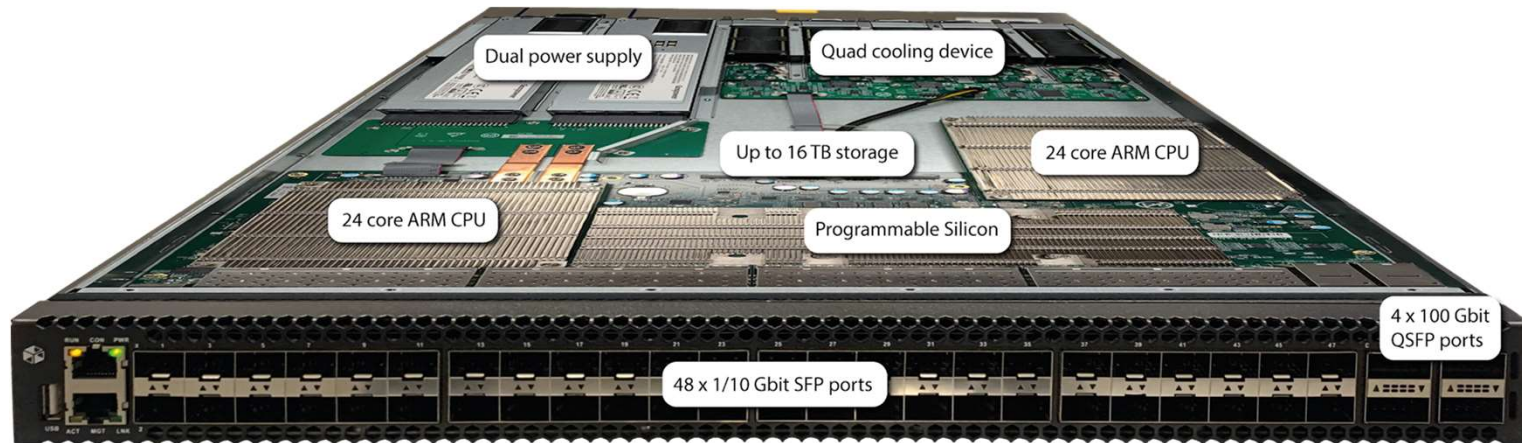
Estimated IPFIX Metadata retention time

Bandwidth in Gbit/s	1	5	10	30	60	90	Retention time in days
0,1	0,060	0,180	0,330	0,990	1,950	2,940	
0,5	0,180	0,810	1,620	4,860	9,720	14,040	
1	0,330	1,62	3,240	9,720	19,440	29,160	
5	1,62	8,10	16,20	48,60	97,20	145,80	
10	3,24	16,20	32,40	97,20	194,40	291,60	
50	16,20	81	162	486	972	1.458	
100	32,40	162	324	972	1.944	2.916	
500	162	810	1.620	4.860	9.720	14.580	
1000	324	1.620	3.240	9.720	19.440	29.160	in TB storage

Estimated Cubro Metadata retention time

Bandwidth in Gbit/s	1	5	10	30	60	90	Retention time in days
0,1	0,00	0,014	0,029	0,086	0,173	0,259	
0,5	0,01	0,072	0,144	0,432	0,864	1,296	
1	0,03	0,14	0,29	0,86	1,73	2,59	
5	0,29	1,44	2,88	8,64	17,28	25,92	
10	0,72	3,60	7,20	21,60	43,20	64,80	
50	1,44	7,20	14,40	43,20	86,40	129,60	
100	2,88	14,40	28,80	86,40	172,80	259,20	
500	14,40	72	144	432	864	1.296	
1000	28,80	144	288	864	1.728	2.592	in TB storage

Cubro Omnia 120: powering DPI for Stablenet



Omnia 120 is an Enterprise Visibility node with high end L7 packet forwarding silicon, in combination with two ARM multicore CPUs for advanced visibility and security applications.

The unit comes with 48 x 10/1 Gbit SFP and 4 x 100/40 QSFP or 4 x 4 10/25 Gbit with breakout.

Each of the two ARM CPUs are connected via a full duplex 100 Gbit interface for maximum application performance.

Interworks with existing Visibility installations or Cubro provided Visibility solution

60GB/sec of DPI performance

Thank

