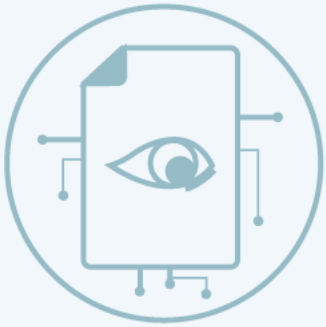
CUBRO
NETWORK VISIBILITY



OMNIA SEC

SOLUTION BRIEF

JANUARY 2024

CUBRO
NETWORK VISIBILITY

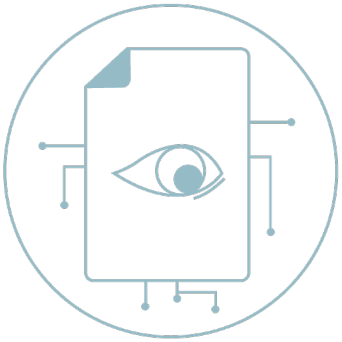


TABLE OF CONTENTS

Introduction

Cubro's specialized Omnia SEC solution elevates application and subscriber-aware filtering to another level. It is tailored to optimize cybersecurity feeds for Communication Service Providers (CSPs) and specifically tackles the central challenge of reducing traffic to enhance cybersecurity measures. Our effective and resilient approach transforms data management, ensuring efficiency without compromising resources. It provides a scalable solution adept at managing extensive traffic volumes, reaching several terabits per second (Tbps).

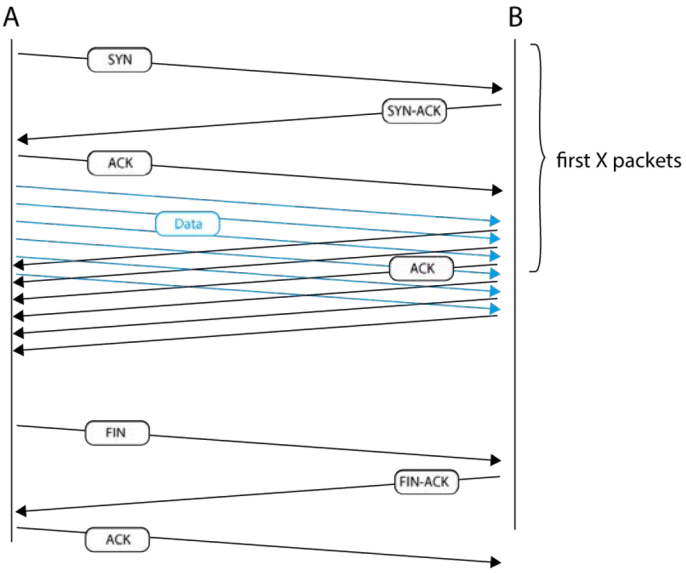
Application filtering

Cubro's advanced Deep Packet Inspection algorithms are trained to recognize video and streaming media and, if desired, remove these network flows from inspection by any tools that don't add value. The application filtering mechanism can recognize feeds such as YouTube, Facebook, Netflix, and other "Over the top" applications, even when these feeds are accessed via web browsers, or the protocols use encryption technology -- and then remove these streams before they are sent to various network security tools.

Beyond the source, destination, duration, quantity, and actual application driving the network flows, Cubro's deep packet inspection can give you the Geo-location of the parties and the reputation of the sender or receiver indicating whether the traffic might be malicious.

Flow sampling on TCP traffic

Cubro introduces a second filter stage through TCP/IP packet flow sampling. We forward only the initial 10 to 15 packets (configurable) to the security tools, which is typically sufficient for detecting malicious traffic and activities.



Enrichment of subscriber data (ISP)

Correlation is essential because most security tools deal with only IP addresses and in a service provider network the IP address is not a unique identifier for the subscriber. Depending on the network type, Mobile or fixed, Cubro offers solutions to identify the subscriber by correlating/mapping signaling information to the cybersecurity event.

Geo Events

Cyber security events will be enriched with the subscriber's geo location data producing heat maps of affected areas.

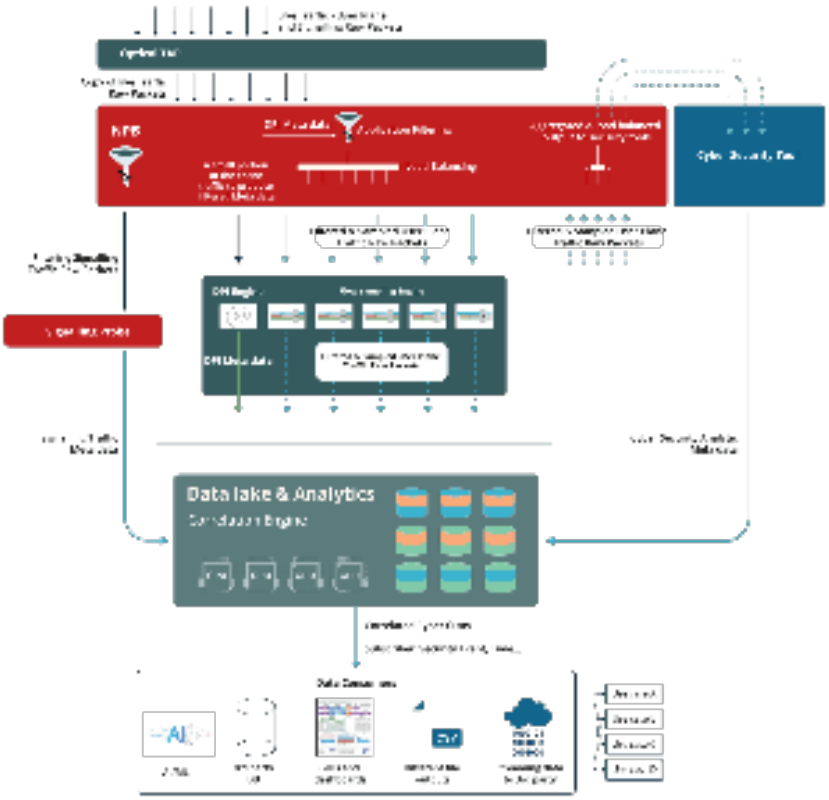
Solution for small and big networks

Cubro offers a scalable solution designed specifically for the networks of small and mid-sized enterprises, including expansive service provider networks. The unique advantage of Cubro's solution lies in its cross compatibility of software and hardware, enabling the seamless execution of essential services within an Omnia120 Network Packet Broker and a compact server. This innovative approach caters particularly to customers dealing with a limited volume of data and constrained rack space.

For larger Internet Service Providers (ISPs), Cubro's SmartNIC technology, embodied in the Cubro Omnic, stands out as a cutting-edge solution. Leveraging this advanced technology, ISPs can harness highly optimized software to achieve the remarkable capability of processing terabits of user data every second. This unparalleled performance underscores Cubro's commitment to delivering sophisticated and efficient solutions that meet the evolving demands of modern network infrastructures, ensuring both scalability and optimal functionality.

Solution Description

- Traffic comes from TAP/s or already existing Network Packet Broker (NPB).
- Signalling traffic is directed to Signalling probe (Signalling probe provides metadata to perform mapping IP and subscribers sent to the data lake).
- A fraction of the traffic sent to the DPI engine on Omnic. The DPI engine extracts metadata for application filtering.
- NPB removes all non-relevant traffic and load balances the traffic to several Omnics where the TCP/IP flow sampling is conducted.
- Traffic is sent back to NPB for aggregation. The second load-balancing stage is to feed the cybersecurity tool.
- The cybersecurity tool processes the remaining traffic and sends metadata to the Cubro Data Lake.
- In the data lake, the signalling and the security metadata are correlated/ mapped, and maybe enriched with other 3rd party data.
- This is the final usable data stream for the Service Provider.



Key Use Cases

Cyber security bundles for subscribers

Offer security packages to subscriber to protect end devices, secure your customers data and enhance the overall user experience.

Optimize Flow monitoring

Reduce the bandwidth for older and costly flow monitoring solutions without taking any compromises in the quality of your reports.

Geographical Attacks

By mapping the geographical locations of affected subscribers, Cubro successfully pinpoints potential cyber-attacks, enabling swift and targeted response measures to safeguard both the network infrastructure and the subscribers in the affected areas. This proactive approach not only enhances the security posture of the telecommunications ecosystem but also underscores the significance of geolocation in detecting and mitigating cyber threats.