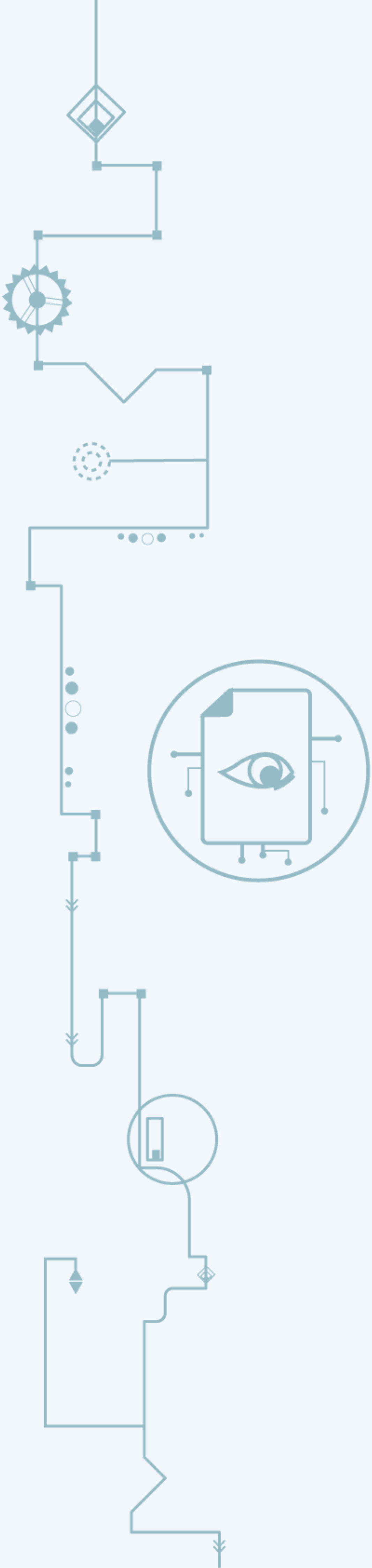
CUBRO
NETWORK VISIBILITY



OMNIA SEC

SOLUTION BRIEF

JANUARY 2024

CUBRO
NETWORK VISIBILITY

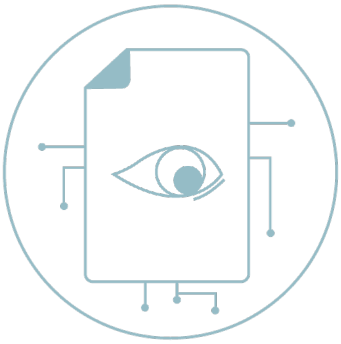


TABLE OF CONTENTS

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).

SEC OMNIA

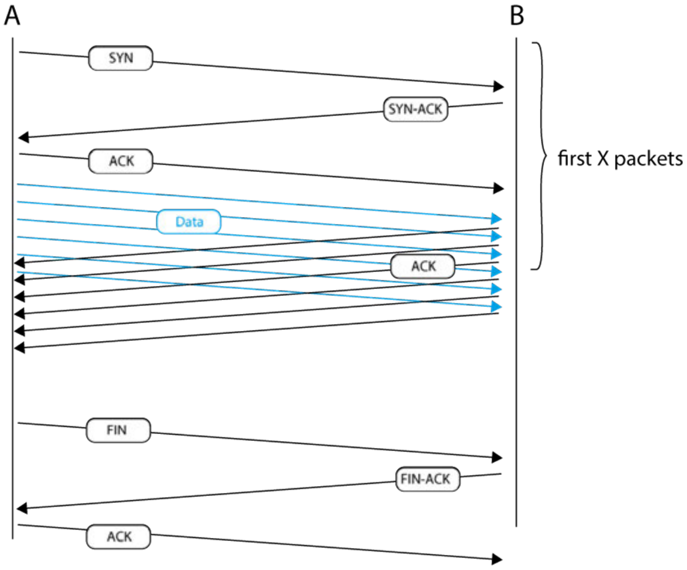
Application filtering

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.

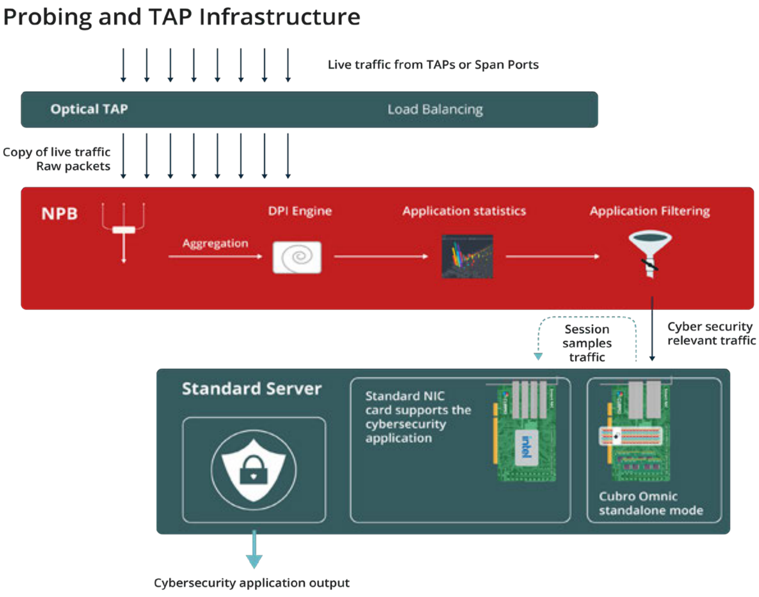
Solution for small and big networks

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 TAPs or already existing Network Packet Broker (NPB). In this example, Omnia120 aggregates the different input ports.
- The aggregated traffic is 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 if needed where the TCP/IP flow sampling is conducted.
- This Omnic can be installed in any server or in the actual server where the cybersecurity solution is running. This is possible because the Omnic runs in standalone mode and only requires power from the server, no software is needed.
- The sampled traffic is then sent to Server NIC where the Cyber tools do their work.
- This is a very efficient way to lower the cost of any kind of cybersecurity solution.


Probing and TAP Infrastructure
Live traffic from TAPs or Span Ports
Optical TAP
Load Balancing
Copy of live traffic
Raw packets
NPB
Aggregation
DPI Engine
Application statistics
Application Filtering
Session samples traffic
Cyber security relevant traffic
Standard Server
Standard NIC card supports the cybersecurity application
intel
Cubro Omnic standalone mode
Cybersecurity application output

Key Use Cases

Reduced data overhead

Cubro's TCP session slicing allows for the extraction of only the relevant parts of network traffic, reducing the amount of data that needs to be processed and stored. This helps in optimizing resources and improving overall efficiency. Reduction in the overall cost of cybersecurity solution.

Optimize Flow monitoring

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

Increased threat detection & faster response time

The Cubro solution removes unnecessary data for Cyber Security tools, increasing their detection rate & response time, lowering retention time and, lowering license fees.