

Joint components

- **Cubro layer 1 products** — optical TAPs and breakout boxes for passive access to physical links.
- **Cubro network packet brokers** — including the SessionMaster series, with header modification, packet slicing and session-aware load balancing, so each tool receives only the traffic it needs.
- **Uila virtual taps** — East/West capture between VMs on the same host and across hosts in the data centre.
- **Uila cloud capture** — the same view of workloads running in public cloud environments.

Where the traffic comes from

East/West between VMs on one host. East/West between hosts across the distributed virtual switch. North/South at the physical network edge. Workloads in public cloud.

Four sources, one packet broker, one feed to your tools.

Also available

- **Cubro bypass switches** — keep the link up when an inline security tool needs maintenance or fails.

The visibility gap in virtual environments

Most traffic in a modern data centre never crosses a physical link. It moves between virtual machines on the same host, or between hosts across a distributed virtual switch, where TAPs and SPAN ports cannot reach it. Packet data is still the basis of performance troubleshooting, forensic investigation and threat hunting. In virtualised and cloud environments, collecting it has usually meant manual work across several disconnected tools.

Cubro and Uila close that gap together. Uila virtual taps capture East/West traffic inside the virtual environment, including workloads in public cloud. Cubro TAPs and network packet brokers capture North/South traffic in the physical network. Both streams meet in the packet broker, where they are aggregated, filtered and optimised before they reach the monitoring and security tools.

The tools then see the full path of a transaction instead of one segment of it. Detections carry fewer false positives, and the metadata an analyst needs is already in place when an incident starts.

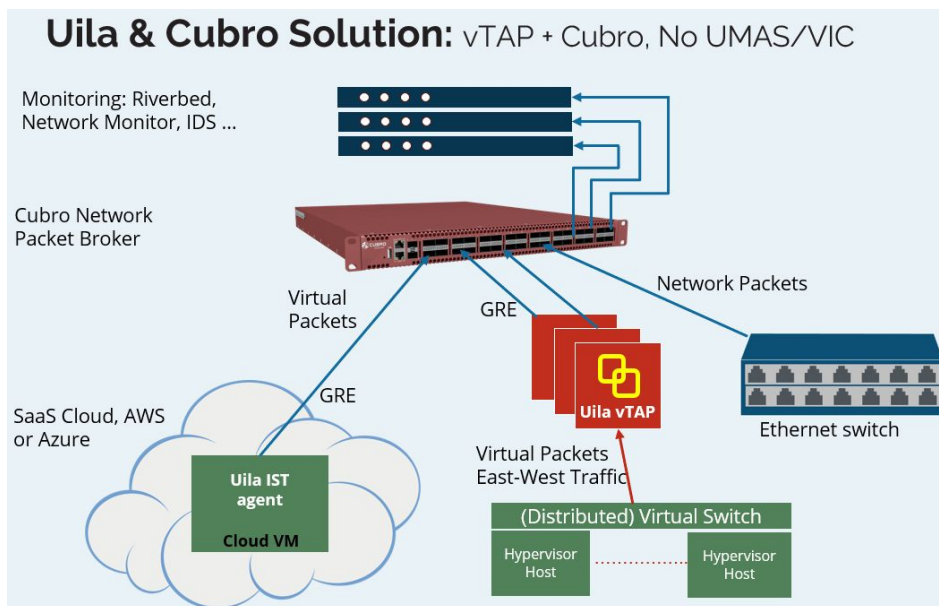


Figure 1: Uila virtual taps and Cubro packet brokers feeding one monitoring layer.

What the combination delivers

- One feed containing East/West, North/South and cloud traffic.
- Less traffic per tool, without losing session context.
- No change to the monitoring and security platforms already in place.

How the joint solution works



1. Capture. Uila virtual taps copy East/West traffic inside the virtual environment: between VMs on a host, between hosts across the distributed virtual switch, and in public cloud deployments. Cubro TAPs copy North/South traffic passively at layer 1, with no effect on the production link.

2. Aggregate. Both streams arrive at a Cubro network packet broker, which combines them into a single view of the network with physical and virtual traffic side by side.

3. Optimise. Filtering, deduplication, packet slicing and header modification cut the volume before it reaches a tool. Session-aware load balancing then spreads traffic across tool instances without breaking flows, so a session always lands on the same analyser.

4. Deliver. The optimised feed goes to the application monitoring, network monitoring and IDS platforms already in place. Nothing needs replacing.

What changes for the operations team

Blind spots close, and tools that were already paid for start seeing the traffic they were bought to analyse. Because the packet broker removes duplicate and irrelevant packets first, the need for extra tool capacity and licences grows more slowly — often the part of the business case that pays for the deployment.

Typical deployment

A virtual tap per hypervisor host, Cubro TAPs at the physical links that matter, and one packet broker in front of the monitoring layer. The design scales by adding taps and broker ports rather than by rebuilding the monitoring architecture.

Why Cubro TAPs and packet brokers with Uila

- **Strong features-to-price ratio** — technically elegant designs, priced so the business case does not need defending twice.
- **Advanced capabilities as standard** — session-aware load balancing, header modification and packet slicing, not chargeable extras.
- **Low cost of entry** — straightforward to budget for, deploy, expand and operate.
- **Support in your time zone** — Cubro engineers answer directly, wherever the deployment sits.
- **European engineering** — developed and supported from Vienna, with sales presence in all time zones.
- **Decades of engineering experience** — widely deployed and proven with service providers and enterprises.
- **No competitive overlap** — Cubro does not sell NDR or TLS 1.3 decryption products. Your choice of security tools stays your choice.
- **Commercial and technical flexibility** — easy to do business with, from evaluation through to expansion.
- **One integration** — Uila virtual taps feed Cubro packet brokers directly, with nothing custom to maintain.

Where customers use it

Application performance in virtual data centres. When one transaction crosses several VMs, the packet data has to follow it. The joint solution gives the monitoring platform every hop, not only the hops that touch a physical port.

Incident response and forensics. Analysts get East/West packet data and metadata from inside the virtual environment, so lateral movement between workloads is visible during the investigation rather than after it.

Cloud migration. The same capture method applies before and after a workload moves, which makes performance comparison measurable rather than anecdotal.

Tool consolidation. Filtering and deduplication in the packet broker reduce the traffic each tool has to process, and session-aware load balancing lets several tool instances share the load.

Service provider infrastructure. Virtualised core and NFV environments get the same packet-level visibility as the physical network.

At a glance

- **Traffic covered** — East/West, North/South and public cloud.
- **Deployment** — a virtual tap per hypervisor host, Cubro TAPs at the physical links, one packet broker in front of the tools.
- **Tools fed** — application monitoring, network monitoring, IDS, packet capture and forensics platforms.
- **Impact on production** — Cubro TAPs are passive at layer 1; nothing sits inline in the data path.
- **Scaling** — add taps and broker ports; the monitoring architecture stays as it is.
- **Support** — Cubro engineers in Vienna and offers support across all time zones.

About Cubro

Cubro Network Visibility manufactures network TAPs, advanced network packet brokers and bypass switches for telecom and enterprise networks. Cubro is headquartered in Vienna, Austria, and supplies service providers and enterprises worldwide, with offices in Austria, Singapore and the United States and technical support delivered from local time zones.

About Uila

Uila resolves complex IT disruptions for enterprise organisations with its application-centric, full-stack observability platform. The platform correlates application and infrastructure performance to isolate and remediate issues before they affect the business.



Cubro Network Visibility
EMEA USA APAC
sales@cubro.com