CUBRO
NETWORK VISIBILITY

Maximizing Cybersecurity Efficiency: How Network Visibility Improves Security Posture of Enterprises

Ebook

Table of contents

Introduction: The Realities of Cybersecurity in the Enterprise World

Since enterprises have started to use the cloud more extensively, the network environments have become more challenging to monitor and protect. Traditional tools often struggle to keep up with this scale and complexity, leading to inconsistent visibility and potential blind spots.

What is Cybersecurity Monitoring?

Cybersecurity monitoring is the automated process of collecting and analysing indicators of potential security threats and triaging them with appropriate action.

Security operations teams have an ever-increasing amount of work and responsibility in maintaining the overall health, performance, and security of a business's infrastructure as technologies evolve, complexity increases, and enterprise networks continue to grow.

The High Cost of Data Breaches

Today, cybersecurity monitoring is part of a company's compliance and regulatory requirements. Data breaches can be costly: ransom cost, fines and compensations, bad publicity, lower brand value and paused operations preventing business activities. Some of these can have a long-lasting impact on the company, including lowered stock value.

Network cybersecurity monitoring's core objective is to minimise downtime by preventing attacks and preserving data to keep an organisation operational. By combining attack and passive security monitoring and automating the processes as much as possible, organisations can protect themselves from network threats and identify attackers.

CUBRO
NETWORK VISIBILITY

Common Cybersecurity Pain Points in Large Enterprises

Several tools are on the market for security departments or security operations centres (SOC). SOC is the team and infrastructure responsible for managing an organisation's security posture, leveraging tools like SIEM and SOAR. Security information and event management (SIEM) collects and analyses security data, identifying potential threats. Security orchestration, automation and response (SOAR) automates and orchestrates responses to security incidents, improving SOC efficiency.

Network detection and response (NDR) refers to a category of network security products that detect abnormal system behaviours by continuously analysing network traffic. Endpoint Detection and Response (EDR) is used for unusual activity on system endpoints, including computers, phones, and servers.

Network and security monitoring provide comprehensive information, analysis, and reports. The aim is to automate these functions as much as possible.

Enable network operations and network security staff to collect, filter, and refine their investigations to identify problems.

Determine if the event is a normal network or malicious/disruptive activity.

Provide continuous, real-time, and reliable data gathering for extracting crucial information about the health and security posture of the network.

Deploy active testing tools to test vital network functions.

Allow automation and standardised trouble ticketing processes.

Automation tools, particularly agentic AI, help make these tasks easier.

CUBRO
NETWORK VISIBILITY

Finding the Right Balance

On the one hand, it is tempting to choose the best of breed tools to create a best of industry service operation centre, but integrating them always comes with a cost. On the other hand, one vendor solution minimises the integration costs, but the risk of vendor lock-in is not appealing. Often, one vendor solution is criticised for its limited agility. NPBs increase flexibility by sending the same or filtered traffic to several destinations. This enables using tools in parallel, for example, when testing and comparing tools to each other or when having tools for specific purposes.

Another area where TAP and NPB are helping is traffic reduction and filtering to choose only relevant traffic to remove performance bottlenecks. Security tools may require continuous HW and license upgrades with increasing traffic.

In either case, it is important to have all the necessary data for the tools.

Regardless of what kind of solution is chosen, cost monitoring is essential. The cost overruns are due to licensing, bandwidth charges, and inefficient use of tools. The number of servers often impacts the licensing fees, and sometimes upgrading the HW and reducing the number of servers can create substantial savings. Bandwidth and efficient use of the tools can be favourably improved by using TAP and NPB solutions.

CUBRO
NETWORK VISIBILITY

The Invisible Layer That Holds It All Together – Why Network Visibility is the Backbone of Modern Cybersecurity

Why Network Visibility is the Backbone of Modern Cybersecurity

In a world overflowing with security tools, dashboards, alerts, and automation, there's one critical layer that's often overlooked - 'Network Visibility'.

What Network Visibility Is

The ability to see, monitor, and analyse all network traffic - from raw packets to metadata - in real time.

A foundational capability that provides complete visibility into east-west and north-south traffic across physical, virtual, and cloud environments.

An independent source of truth; feeding accurate traffic data to security, performance monitoring, and analytics tools.

What Network Visibility Isn't

Firewall, IDS/IPS, or SIEM do not provide visibility but are consumers of visibility.

It's not another point solution to be added to the already overcrowded security stack.

It doesn't create traffic noise - instead, it filters, directs, and enriches traffic data to help other tools work better.

Cubro: The Enabler, Not the Enforcer

At Cubro, we don't compete with your security tools - we make them stronger. As a vendor-neutral enabler, our job is to:

Deliver clean, filtered, and relevant traffic to the right tools at the right time.

Optimising the use of tools by avoiding duplicate processing across platforms.

Improve ROI on existing investments by ensuring that every security tool sees what it’s supposed to see.

Bridging the Gap Between IT and Security

Network visibility isn’t just about technology - it’s about collaboration.

IT operations and security teams often operate in silos, using different tools and chasing different goals.

With Cubro’s centralised visibility fabric, both teams get access to the same underlying traffic, reducing miscommunication and accelerating incident response.

This shared visibility layer becomes a unifying platform for performance monitoring, threat detection, forensics, and compliance.

Test Access Point (TAP), Network Packet Broker (NPB) and advanced NPB

Both TAPs and NPBs are fundamentally important in providing visibility to the network by providing a copy of packets traversing the network.

TAP is a stand-alone piece of hardware that mirrors packets by making an exact copy of the traffic ensuring that total visibility is provided across all of the network's security and monitoring platforms.

NPB optimises the traffic between TAP and monitoring systems. Also known as Traffic Aggregator, an NPB improves the functionality of network analysis and security tools, helps to optimise network security and the performance of monitoring and analysis tools by decapsulating tunnelling protocols, slicing packets if needed, aggregating, filtering, replicating and load balancing.

Advanced NPBs generate metadata and provide a basic security view.

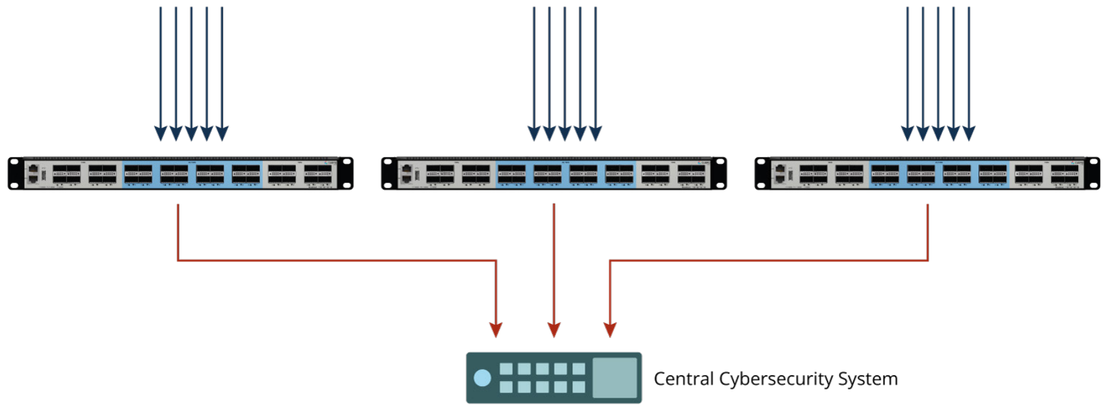
While network monitoring can cope with information received from network elements, many other tools require packet information. This is where network visibility becomes essential, since without tapping and NPBs the information from the network is not complete or even useful. NPBs play another important role in optimising, reducing and formatting the data for the monitoring tool, thus reducing the investment needed.

How Cubro Solves These Challenges

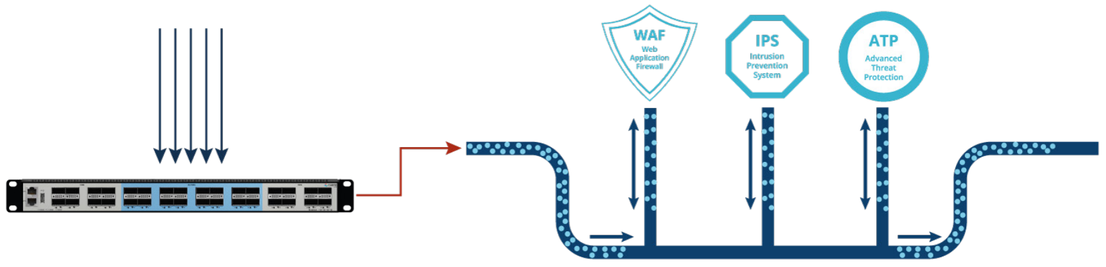
Enterprises have a wide selection of solutions to choose from. However, today's best solution may not remain optimal in the future due to evolving business needs and the continuous advancement of cybersecurity technologies. Ideally, enterprises should be able to run multiple tools in parallel, stay vendor-agnostic, and remain future-proof.

Cubro's network packet brokers (NPBs) and bypass appliances support this approach in several ways:

Simplified branch and central office deployment: Aggregating and filtering traffic at branch offices before forwarding it to a central location can reduce complexity and cost.



Seamless migration: When migrating to a new cybersecurity system, avoiding downtime is essential. Bypass and NPB solutions allow traffic redirection, ensuring uninterrupted visibility during the transition.

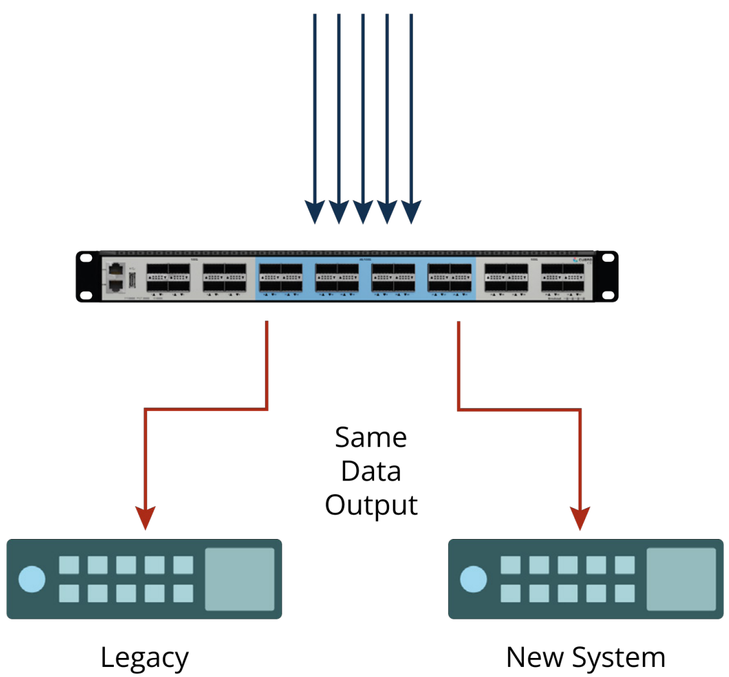


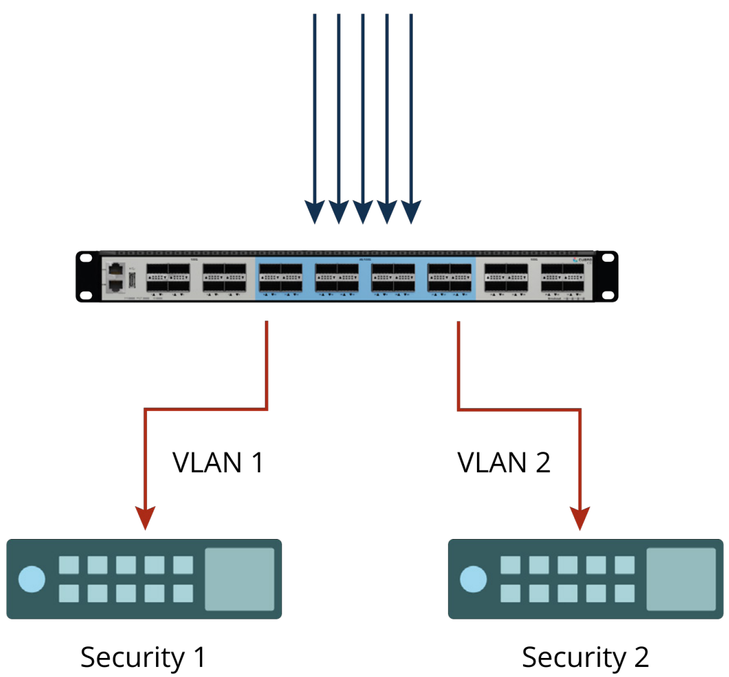
Cubro solves Challenges

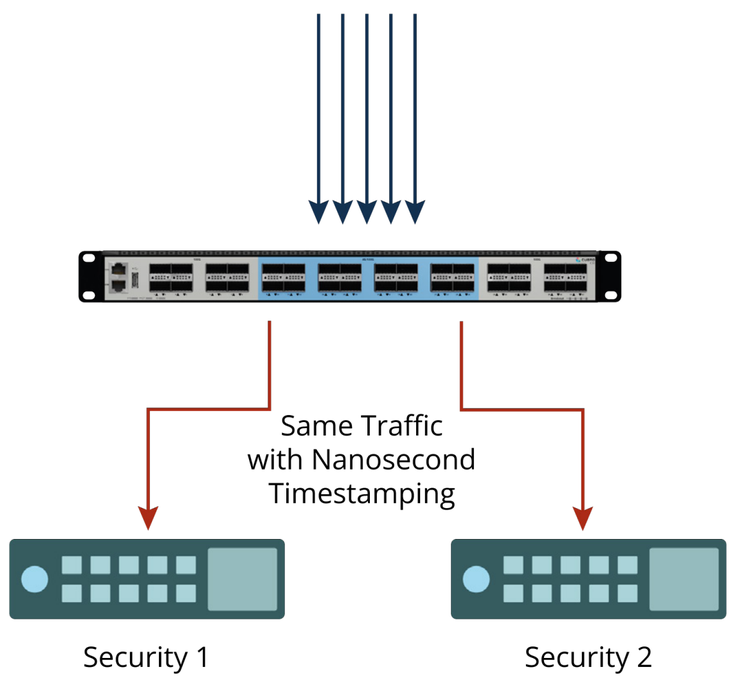
Support for legacy and next-gen tools: The same Cubro infrastructure enables concurrent use of both legacy and modern security tools, aiding benchmarking and comparative analysis.

Selective data forwarding: Enterprises often use multiple tools for specific tasks. Tag-based segmentation (e.g., VLAN or VXLAN) ensures that only relevant data is delivered to the appropriate tool.

Time-based comparison: For evaluating security tools, time synchronization is a valuable metric. Cubro provides nanosecond-level timestamped traffic for accurate, time-based tool comparison.







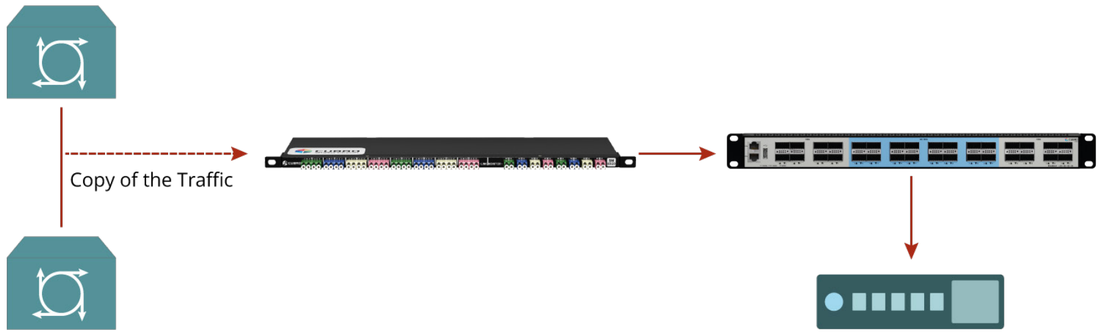
Cubro solves Challenges

Cybersecurity cost optimisation from Day One, with improved performance and response times - without impacting live traffic.

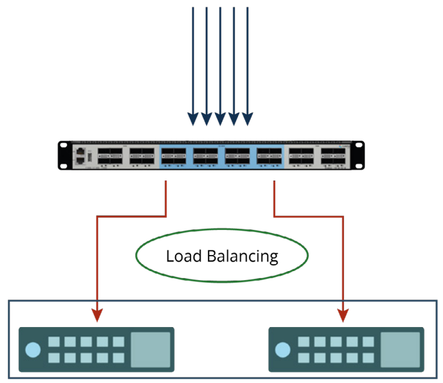
The previous section explained how Cubro supports evaluating and selecting security solutions. This section focuses on the integration phase - optimising costs and performance from the start, while preserving live traffic integrity.

Key techniques include:

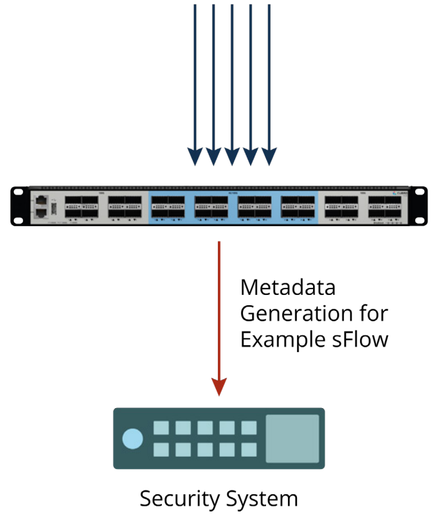
TAP-based traffic access: TAPs create passive copies of live traffic without affecting network performance. Captured traffic is typically routed through an NPB for further processing.



Session-aware load balancing: Efficiently distributes output traffic across multiple input cards of a tool, ensuring optimal performance.

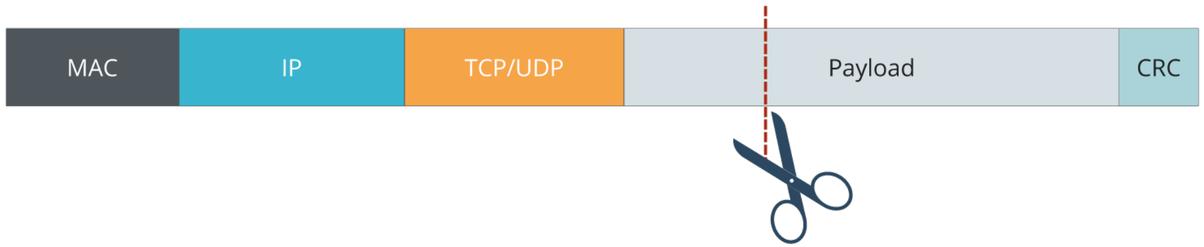


Metadata generation: When tools accept metadata, Cubro's support for metadata generation can significantly reduce traffic volume - although full-packet inspection is still required by many security systems.

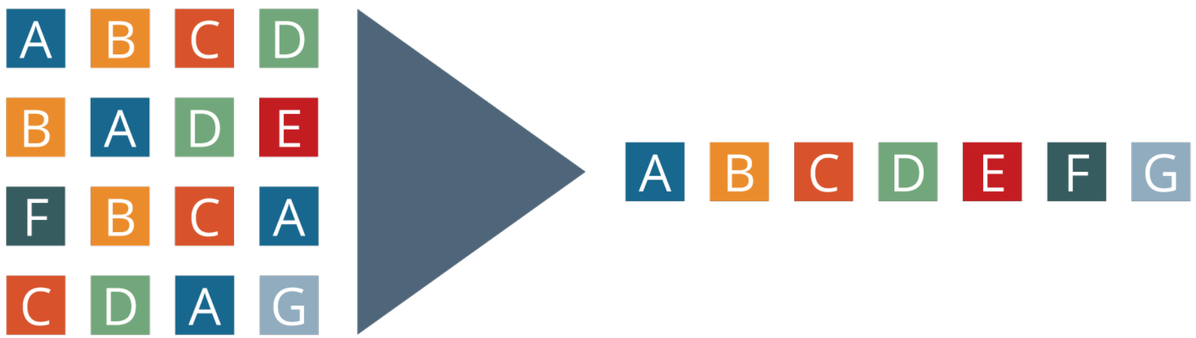


Cubro solves Challenges

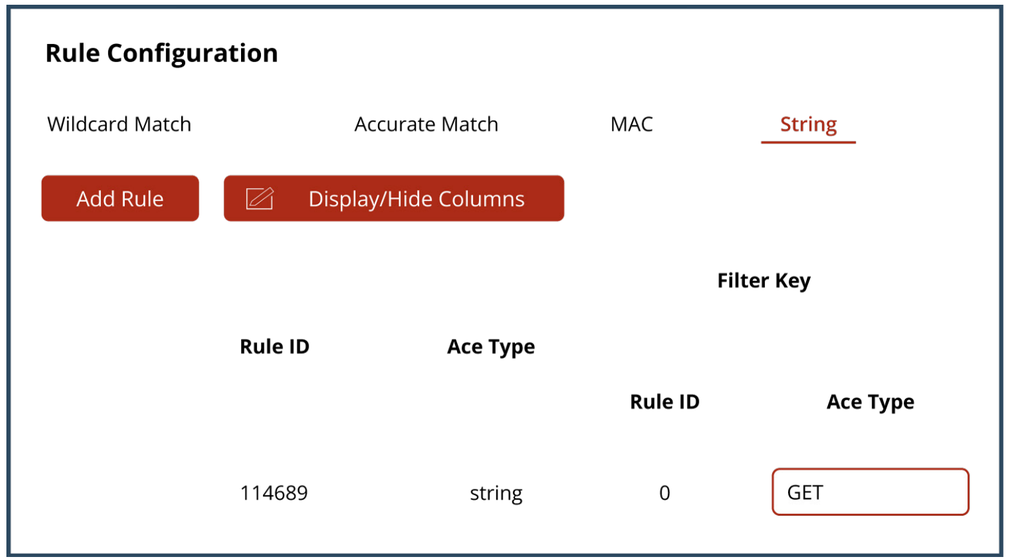
Packet slicing: If the analysis focuses on user-plane data, packet slicing can yield substantial reductions in data volume and improve search speed. For example, an NPB can isolate HTTP GET traffic - a capability especially useful in intrusion detection scenarios.



Duplicate packet removal: Removing redundant packets is another method to decrease unnecessary data.



Advanced filtering: Filtering based on IP addresses, ports, protocols, tunnel identifiers, or pattern matching can dramatically reduce data volume and improve search speed. For example, an NPB can isolate HTTP GET traffic - a capability especially useful in intrusion detection scenarios.



Use Case 1

Cybersecurity Use Cases

Case Study 1: Reducing SIEM costs by filtering irrelevant traffic before ingestion.

Leading Financial Institution Optimises Performance of Security Software
Industry: Enterprise (Financial Services)

Challenge

A Japan-based financial institution with 20 branch offices and over 2000 employees needed to integrate a Trellix security solution across its network. Key issues included:

- High tool costs due to the growing monitoring points
- Limited availability of aggregation devices (1000Base-T)
- Lack of centralised visibility
- Inefficient use of security tools due to irrelevant traffic ingestion

Solution

Cubro deployed its EX5-3 Network Packet Broker in remote data centres to:

- Aggregate and filter traffic from branch offices before forwarding it to the central Trellix solution
- Generate sFlow data for further analysis
- Eliminate blind spots and reduce tool overload
- Enable centralised management of security software

Results

- Reduced SIEM and security tool costs by filtering out non-relevant traffic
- Increased efficiency of the Trellix solution through optimised traffic flow
- Improved ROI by reducing required monitoring interfaces and consolidating tools
- Enhanced visibility and security with no impact on live network traffic
- Scalable and fail-safe deployment across multiple data centers

Use Case 2

Case Study 2: Enabling smooth transition between security vendors in a multinational rollout

Global Enterprise Ensures Seamless Migration with Cubro Network Visibility | **Industry:** Enterprise / Multinational Corporations

Challenge

A global enterprise operating across North America, Europe, and Asia planned to transition from a legacy security solution to a new, next-generation security vendor as part of a phased, multinational rollout. The primary challenges included:

- Need to maintain uninterrupted visibility during the migration
- Ensuring simultaneous support for both legacy and new security tools
- Sending the same data to several destinations, filtering, and forwarding across geographically dispersed data centres
- Minimising downtime, tool overlap costs, and operational complexity

Deployment Approach

- Installed Cubro devices in all major regional data centres
- Used traffic filtering to reduce load and tailor feed to specific vendor formats
- Enabled both old and new security solutions to coexist during testing and verification phases
- Centralised traffic aggregation for streamlined tool deployment and visibility

Solution

Cubro provided a vendor-agnostic visibility layer using a combination of its Network Packet Brokers EXA32100A and bypass technology, allowing the customer to:

- Duplicate and filter traffic for both old and new security tools in parallel
- Segment monitoring zones per region with centralised management and control
- Use traffic forwarding to direct relevant data to appropriate tools based on the stage of deployment
- Enable fail-safe failover mechanisms to ensure tool availability during cutovers

Results

- Zero downtime during vendor migration phases
- Seamless co-existence and validation of a new security vendor across regions
- Significant cost savings by avoiding redundant tool usage and reducing traffic loads
- Improved operational efficiency with central control over the tool transition process
- Flexibility to scale or repeat the transition framework for future vendor changes

Use Case 3

Case Study 3: Running parallel NDR and IDS tools with identical traffic for evaluation.

Defense Organization Ensures Robust Cybersecurity Evaluations with Cubro Visibility Solutions
Industry: Defence / Government / National Security

Challenge

A national defence organisation required a seamless evaluation of new Network Detection and Response (NDR) solutions while operating its existing Intrusion Detection System (IDS) for real-time security monitoring. Given the sensitive nature of national security operations, the key challenges included:

- Ensuring parallel operation of legacy IDS and new NDR tools without interrupting ongoing defence operations
- Maintaining full traffic visibility across critical defence network environments without packet loss or degradation
- Handling complex traffic while ensuring the tools could process data accurately
- Implementing vendor-agnostic solutions to evaluate multiple security vendors for best-fit options

Solution

Cubro delivered a high-performance visibility layer using its advanced Network Packet Brokers EXA64100 and Network TAPs, which:

- Sent the same network traffic to several destinations to simultaneously feed both the legacy IDS and the new NDR solution, ensuring accurate and effective evaluation
- Applied intelligent filtering to eliminate unnecessary or irrelevant traffic, especially when dealing with sensitive military communications
- Allowed the defence organisation to run both tools in parallel without any risk to national security operations
- Offered seamless integration into the defence organisation's existing security infrastructure, providing centralised control over evaluation tools across multiple regions

Use Case 3

Deployment Highlights

- Cubro devices were installed in critical data centres across strategic locations to aggregate and manage high volumes of sensitive military data.
- Deployed advanced traffic filtering and load balancing, enabling real-time traffic replication with minimal impact on network performance
- Used synchronised time-stamped traffic for precise comparison of security tool effectiveness
- Enabled secure, fail-safe deployment to ensure continuity in defence operations during the evaluation

Results

- Enabled uninterrupted real-time defence operations while running parallel security solutions for evaluation
- Accurate side-by-side comparison of the NDR and IDS systems in detecting and responding to cybersecurity threats in real time
- Reduced evaluation risks and costs by avoiding redundant tool deployments and ensuring effective traffic management
- Enhanced overall cybersecurity resilience, helping the defence organisation select the most effective solution for its long-term national security needs.
- Positioned Cubro as a trusted partner for future military cybersecurity implementations and transitions

Business Value for the C-Suite

- Better Security Outcomes: In line with business needs
  Cybersecurity is a business enabler, and Cubro's solutions help organizations meet industry regulations and internal security policies - protecting their operations from reputational damage and financial loss due to network breaches.

- Better ROI: Cost-efficient cybersecurity strategy.
  Cubro's solutions optimize data feeds to security devices, reducing traffic volume while preserving essential intelligence. This lowers the required size and capacity of security devices, cutting CAPEX and OPEX, and improving ROI.

- Smarter Investments: Spend where it matters most.
  Deploying a Cubro network visibility solution allows an organisation to install network security architectures that allow targeted investments in network security equipment that best suit an organisation's business operation today and evolve as it changes over time.

- Flexibility for the Future: Avoid long-term lock-in.
  Cubro's vendor-agnostic solutions reduce the risk of vendor and technology lock-in so that organisations can maintain the choice of network security products that best meet their network operational needs while minimising costs and maximising return on investment.

The Cubro Difference

Cubro's success comes from experience, innovation, and a focus on what matters most: security, quality, and customer value.

ISO 27001:2022 Certified Operations and Commitment to Security
Our ISO 27001:2022 certification isn't just a stamp of approval- it reflects our daily dedication to protecting both our company and customers. Security is built into everything we do, from operations to product design.

21+ Years of Privately Owned, Debt-Free Innovation
For over 21 years, we've been a privately owned, debt-free company. This allows us to stay focused on long-term innovation, always working to improve and stay ahead in the network visibility field without external pressures.

Global Presence, Local Expertise
We operate globally but always maintain a local touch. Whether you're in North America, EMEA, or APAC, our teams are ready to provide the expertise and support that best fits your specific needs.

Future-Ready: Sustainable Shipping, Virtual Trainings, Customer-Focused Roadmap
Looking forward, we're focused on sustainability and adaptability. With our involvement in DHL's GoGreen Plus program, we're reducing the environmental impact of shipping. We also offer online training to keep customers informed and efficient. And with a roadmap driven by customer feedback, we're always adapting to meet new challenges and opportunities.

Our approach combines the reliability of experience with the flexibility needed to stay ahead in a fast-changing industry.

Discover Our Products and Solutions

Scan the QR code below to explore more about our products and how they can help enhance your network visibility.

If you have any questions or need assistance, feel free to reach out to us at **support@cubro.com**.
Our team is always ready to assist you!