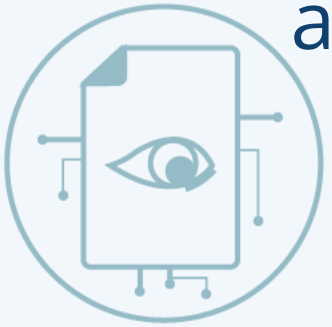
CUBRO
NETWORK VISIBILITY

Enhancing security in critical and industrial **OT networks** with tapping and aggregation solutions



SOLUTION BRIEF

APRIL 2024

Introduction

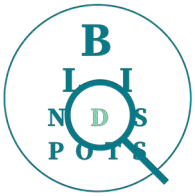
Operational Technology (OT) refers to the hardware and software systems that monitor and control industrial processes, such as manufacturing, energy production, and transportation. These systems are typically used in critical infrastructure and require a high level of availability, reliability, and security. As OT systems become more complex and interconnected, managing and monitoring these networks has become increasingly challenging. Traditionally, OT networks were separate from Information Technology (IT) networks. However, modern industrial environments have shifted to a more interconnected architecture, enabling cyber threats to reach beyond traditional IT assets. Thus, cybersecurity teams are being challenged to secure and manage networks that traverse their entire organization, requiring operational visibility to include the wide variety of OT and IT devices on their networks.

Challenges & Solutions

Network monitoring is one key factor in complying with the latest security regulations. It ensures that security and operational anomalies are detected and thus can be appropriately responded to. It is of utmost importance to spot and troubleshoot networking and communication issues that threaten cybersecurity and reliability.

When implementing these security solutions, OT teams face complex challenges around architecting connectivity throughout these large, and sometimes ageing, infrastructures that weren't initially designed without having network security in mind. **A reliable, powerful and separated network visibility infrastructure that does not influence production traffic is the base of an effective OT network monitoring strategy.** A powerful network visibility infrastructure will deliver all required network traffic to security sensors & probes in the most efficient way, reducing operational complexity and costs.

Benefits of a separate network visibility infrastructure



Complete visibility / Elimination of blind spots:

Cubro TAP devices allow full access to all network traffic without using production network functions like unreliable and complex OT switch mirroring to ensure complete visibility. With minimal effort, network tapping provides comprehensive visibility into OT network traffic, including communication between devices, data flows, and protocol interactions. This visibility is crucial for detecting anomalous behaviour, identifying potential security threats, and gaining insights into operational processes.

Real-time monitoring:

Network tapping enables proactive monitoring and threat detection by capturing network traffic in real time. Security teams can analyze traffic patterns, detect suspicious activities, and respond swiftly to security incidents before they escalate.

Granular analysis:

Network tapping facilitates granular analysis of network traffic, allowing security teams to inspect packets at the protocol level, extract metadata, and conduct deep packet inspection. This level of detail is essential for understanding the nature of security threats and performing forensic investigations.

Easy integration with monitoring tools:

Network Packet Brokers getting traffic from tapping and/or span ports process incoming traffic so that it can be integrated seamlessly with existing monitoring and security tools, such as intrusion detection systems (IDS), security information and event management (SIEM) platforms, and threat intelligence feeds. Traffic distribution, like aggregation of various inputs to one or more outputs/monitoring sensors without having an influence on the data quality, is a prime criterion. Moreover, optimal adaption of network traffic, such as filtering, tunnel removal or deduplication, will protect investments in monitoring tools by forwarding network traffic so the monitoring tool can be used in an optimal environment.

Cubro Solutions for Base-T (copper) OT networks

Cubro offers a wide range of network visibility solutions that deliver easy and safe access to OT and IT network traffic. Copper-based networks using CAT5e, CAT6/6a, and CAT7 cabling are still pervasive today. While high-speed telecommunication focuses on 100G and 400G deployments, many OT networks require visibility solutions for 10/100/1000 copper links.

Cubro Base-T Copper TAPs

Network tapping involves the strategic interception of network traffic for the purpose of analysis, monitoring, and security enforcement. Unlike traditional network monitoring methods that rely on network switches or routers to mirror traffic to a monitoring port, network tapping devices are dedicated hardware appliances inserted into the network infrastructure to copy traffic in real time without introducing latency or disrupting network operations.

Cubro offers a full range of easy to use and reliable TAPs for 10/100/1000 Base-T networks. These copper TAPs allow the uninterrupted passage of full duplex data over standard Category 5/6/7 copper network cables. Featuring auto-negotiating between 10Mbps, 100Mbps and 1000Mbps, these TAPs copy the network signals, including any existing physical errors, to the transmit-only monitoring ports. Available in different chassis versions, it comes with various demands and is a cost-effective and safe solution for small to multi-link deployments.

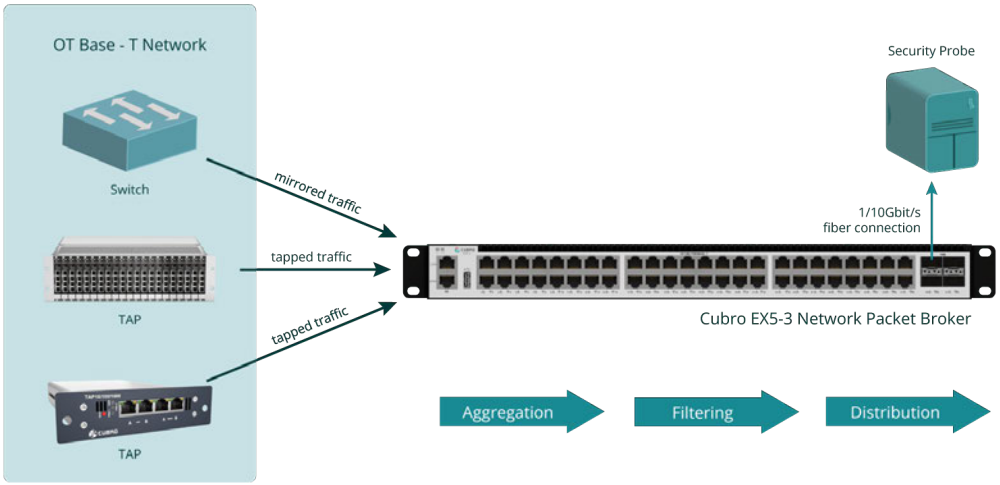
Cubro offers a full range of easy to use and reliable TAPs for 10/100/1000 Base-T networks.

Cubro FlexTAP chassis with up to 21 TAP modules

- Hot expandable at any time without interruption
- Fail-safe design
- Smallest footprint - 21 links in one 19“ 3RU chassis
- Best price and performance
- Redundant & flexible power options (230AV and 48V DC)

Cubro EX5-3 Network Packet Broker

The EX5-3 Network Packet Broker is a high-density solution offering 48 native RJ45 copper ports covering 10M/100M and 1000M. It also provides 4 x 1/10G SFP+ interfaces and thus highlights requirements where fibre-based tools need access to copper-based network infrastructure. Granular filtering options and a straightforward graphical user interface complement the outstanding EX5-3.



Summary

As industries continue to embrace digital transformation and interconnected technologies, the need to strengthen OT security monitoring capabilities becomes increasingly urgent. Proactive monitoring and threat detection are essential for safeguarding critical infrastructure, minimizing operational risks, and ensuring the resilience of industrial systems against cyber threats.

Network visibility offers a powerful means of enhancing OT security monitoring by providing access to network traffic wherever required. By leveraging network tapping technologies and packet brokers, organizations can strengthen their cybersecurity posture, safeguard critical industrial assets, and mitigate the evolving threat landscape in OT environments. As a leading manufacturer and global supplier of network visibility products, Cubro helps customers effectively master OT monitoring challenges.