SOLUTION BRIEF

Cubro with Endace's always-on packet capture delivers total visibility and reliable forensic evidence for robust security.

The Problem

Today's networks face unprecedented threats from sophisticated attackers, and an ever-evolving threat landscape including APTs, ransomware, insider threats, malware and more. The complexity of modern networks and increasing network speeds and loads makes it easier for malicious actors to gain a foothold and avoid detection.

Addressing these challenges requires a comprehensive visibility infrastructure that optimizes traffic for security monitoring tools. Tools can then operate at peak efficiency while performing threat detection, performance monitoring, traffic inspection, or data retention.

Organizations need a solution that:

- Provides full visibility into all network traffic, across the entire network, at high bandwidths and speeds
- Provides efficient capture, filtering, aggregation and de duplication of network traffic so security solutions have access to the most important data
- Integrates with always-on, full-packet capture to ensure all evidence is available
- Provides definitive evidence trail with an accurate record of all relevant packets.

Benefits

- Eliminate network blind spots with comprehensive visibility
- Enable monitoring on high-bandwidth links
- Meet the demands of increasing network speeds
- Streamlined investigation workflows integrated with other tools used by your SecOps and NetOps teams.
- One click access to full definitive packet evidence accelerates investigation and enables accurate reconstruction of events for faster, more accurate incident response.
- Reduced threat exposure through greater analyst efficiency and effectiveness.
- Definitive evidence trail with an accurate forensic record of all network activity.
- High-availability with failover ensures EndaceProbe stacks stay operational when an EndaceProbe is under maintenance.

The Solution

By combining Cubro's leading network visibility solutions with Endace's always-on packet capture, organizations gain comprehensive network visibility regardless of network speeds or loads. Pre-built integrations with a wide range of network security and performance tools, enable faster, more accurate, incident investigation workflows, reducing investigations from hours to minutes or less.

Analysts can access the full packet data related to incidents directly from within their security tools with a single click, enabling fast, easy and conclusive incident investigation and response.

When Cubro's NPBs, switches and TAPs are combined with EndaceProbes customers can precisely record a 100% accurate copy of every network activity – right down to the packet – giving teams ultimate network visibility and definitive forensic evidence.

EndaceProbes capture, index and store network traffic with 100% accuracy while simultaneously providing hosting for a wide variety of network security and performance monitoring tools in Application Dock™, the EndaceProbe's built-in hosting environment.

Cubro's passive network TAPs provide fail-safe access to network traffic. Tapped traffic is forwarded to one or more Cubro Omnia Network Packet Brokers for granular filtering, de-encapsulation of tunneled traffic, de-duplication, decryption, and session-aware load-balancing, optimizing traffic for recording by EndaceProbes and analysis by security tools. Omnia Network Packet Brokers can function as active tunnel endpoints as well as filter on the inner headers of encapsulated traffic. They enable visibility into virtualized network traffic and excel in environments with multiple overlay networks.

Cubro's complete Network Visibility means EndaceProbes can see every packet on the network, enabling them to record a complete history of network activity and give hosted security monitoring tools access to a complete source of traffic for real-time or historical analysis.

Omnia and the EndaceProbe platform both share the ability to host third-party and custom software solutions through Omnia's AppMaster and the EndaceProbe's Application Dock™, offering unparalleled flexibility for deploying network security and performance monitoring solutions.

Conclusion

Combining Cubro with EndaceProbe's always-on, full packet capture delivers a powerful, flexible platform for network security and performance monitoring, providing definitive evidence that enables SecOps teams to resolve complex incidents quickly and accurately across both physical and cloud environments with no blind-spots.

Solution Components

- Cubro TAPs and Omnia Network Packet Brokers
- EndaceProbe Analytics Platforms

How it works

Virtual Extensible LAN (VXLAN) handling on NP8 is most important on overlay Networks

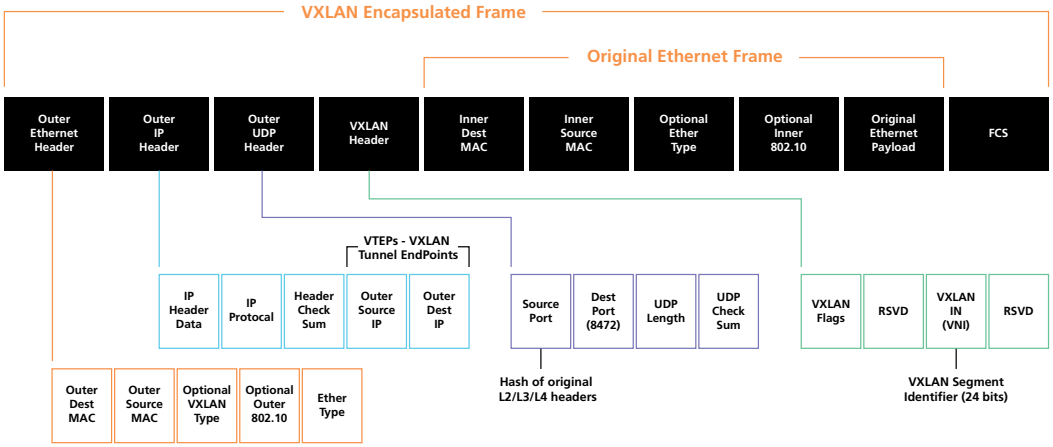


Figure 1: Cubro TAPs passively copy traffic from multiple points in the network and feed the traffic to the Omnia120 Advanced Network Packet Broker. The Omnia120 performs aggregation, de-encapsulation, de-duplication, and traffic filtering as necessary before load-balancing the traffic across multiple EndaceProbe Interfaces enabling complete visibility into network traffic as well as access to high-bandwidth (multiple 100Gbps) links.

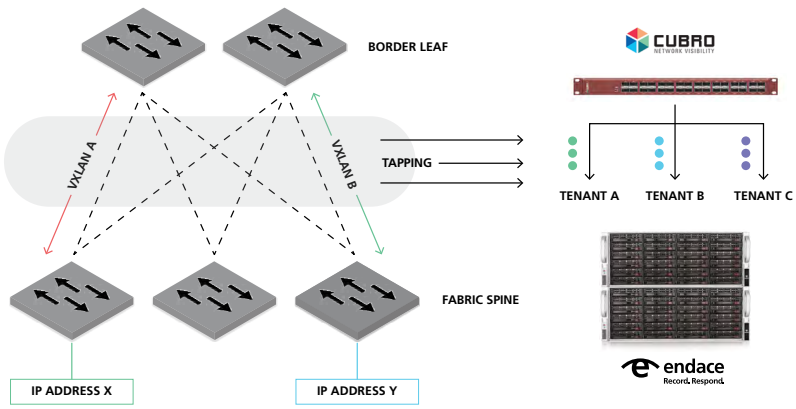


Figure 2: Cubro devices can perform the same function at remote sites, before encapsulating traffic for back-haul to a centralized EndaceProbe deployment.

© 2025 Endace Technology Limited. All rights reserved. Information in this data sheet may be subject to change.

Endace™, the Endace logo, Provenance™ and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

For more information on the Endace portfolio of products, visit: endace.com/products For further information, email: info@endace.com