Cubro & Endace

EndaceProbe and Cubro's Omnia line combine total visibility and traffic recording for robust security.

Today's networks face an unprecedented level of threat from sophisticated, well-funded 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, and while encrypting traffic can help safeguard user privacy it can also create blind spots that attackers can leverage to hide malicious activity such as command-and-control and data exfiltration.

This situation compromises organizations' security postures by increasing the risk of undetected attacks. Addressing these challenges requires a layered approach underpinned by 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.

Cubro is a leading vendor of network visibility solutions that include network TAPs, Advanced Network Packet Brokers, Bypass Switches and Network Probes. Cubro's products remove network blind spots to ensure all relevant network traffic is available for security analysis, while filtering out unnecessary network traffic. They also provide high availability capabilities for security solutions.

EndaceProbe™ Analytics Platforms capture, index and record network traffic with 100% accuracy while simultaneously providing hosting for a wide variety of network security and performance monitoring applications in Application Dock™, the EndaceProbe's built-in hosting environment. Customers can extend their network and security monitoring capability by deploying instances of virtual applications anywhere they have EndaceProbes deployed. Hosted tools can analyze and inspect recorded traffic in real-time at full line-rate or analyze recorded Network History for back-in-time investigation.

Confidently Accelerate Investigations

Cubro Network Visibility complements the EndaceProbe platform with a diverse portfolio of visibility products that deliver comprehensive network access. Visibility starts with Cubro's passive network TAPs, which provide fail-safe access to network traffic. Tapped traffic is forwarded to one or more of Cubro's Omnia Network Packet Brokers for granular filtering, de-encapsulation of tunneled traffic, deduplication, decryption, and session-aware load-balancing, optimizing traffic for EndaceProbe deployments and providing access to high-bandwidth environments. 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.

PRODUCTS

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

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 SecOp and NetOps teams. One-click access to full definitive packet evidence accelerates investigation and remediation and enables accurate reconstruction of events.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Definitive evidence trail with an accurate record of all relevant packets.

Fast, Accurate Security Investigation and Threat Hunting

SecOps analysts can drill down from alarms or threat indicators in their security tools directly to related network packet data in EndaceVision™ or InvestigationManager™ using the EndaceProbe's powerful API integration. The API uses the IP address and time range of the trigger event to focus the analyst directly on relevant incident data. They can then quickly analyze, dissect, and extract the relevant traffic from amongst petabytes of Network History recorded on the network. Analysts can analyze traffic to microsecond level detail with views filtered by Application, IP, Protocol, Top Talkers, and many other parameters, providing rapid insights and enabling accurate conclusions. Being able to get directly to the related packets with a single click enables security analysts to quickly establish the root cause of issues as they are performing investigations or threat hunting in their environment.

Figure 1

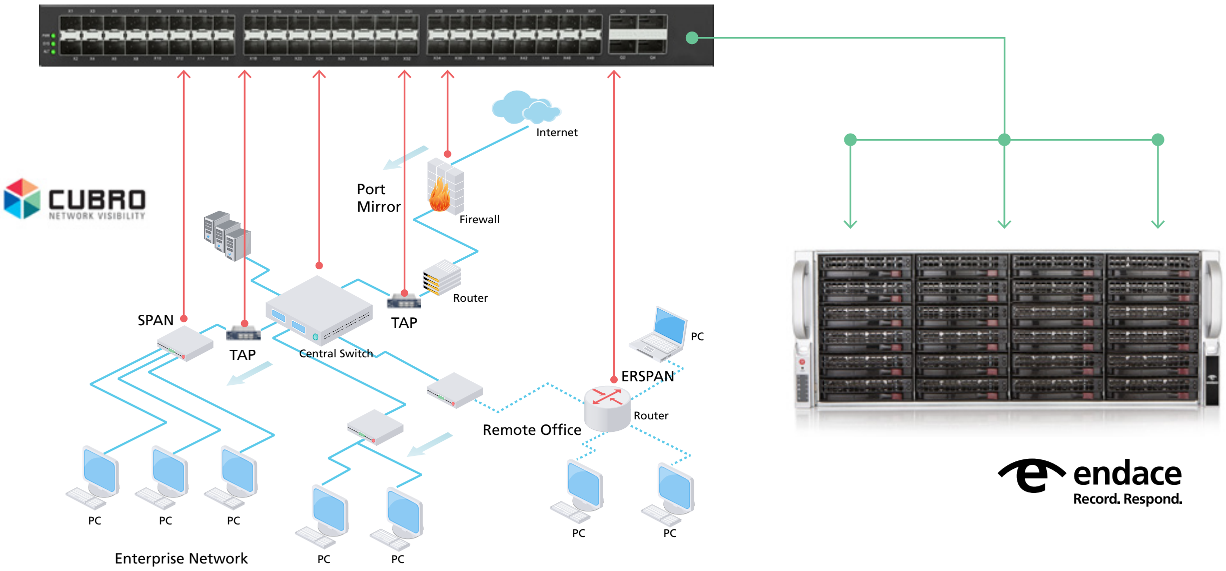
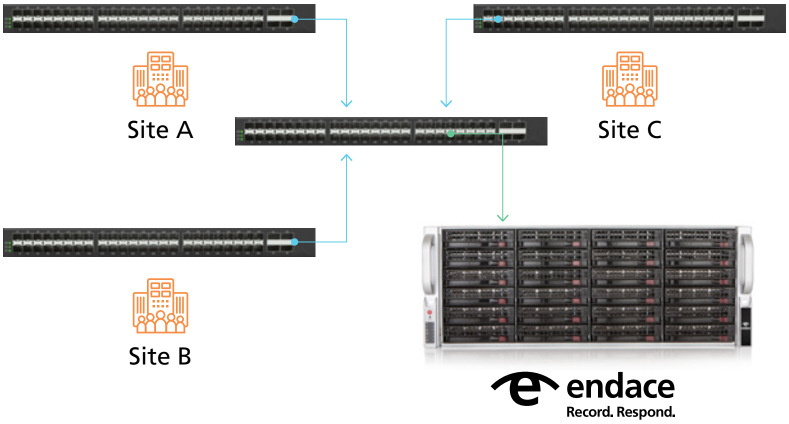


Figure 2



They can respond rapidly to security threats, dramatically reducing the time to resolve critical incidents and minimizing the risk of threats escalating to become more serious breaches.

Omnia and the EndaceProbe platform share the ability to host third-party and custom software solutions through Omnia's AppMaster and the EndaceProbe's Application Dock, offering unparalleled flexibility and integration in any environment.

Use Case or Problem Solved Together

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, deduplication, decryption, 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 backhaul to a centralized EndaceProbe deployment.

Conclusion

Combining Cubro with EndaceProbe's 100% accurate Network History delivers network wide security analytics and always-on recording for definitive evidence that gives SecOps teams the time and forensic data they need to resolve even the most complex investigations faster and more accurately.

Integrating the two technologies allows security teams to respond to alerts faster and investigate threats with more confidence across both their physical and cloud environments, including into encrypted traffic, with no blind-spots. Additionally, the ability to host virtualized security monitoring tools on their EndaceProbes Application Dock or Omnia packet brokers allows customers to extend monitoring coverage and evolve infrastructure quickly to meet new threats without additional hardware deployments, dramatically increasing return on existing infrastructure investments.