JOINT SOLUTION BRIEF

Accelerating Security Investigations: Fortinet, Endace, and Cubro

Joint Components:

- Cubro's layer 1 products including Optical TAPs and Breakout boxes
- Advanced network packet brokers, Sessionmasters, with high performance features including header modification, packet slicing, session-aware load balancing, etc.
- EndaceProbe Analytics Platforms, EndaceVision, InvestigationManager, and EndaceProbe's API integration and Application Dock
- FortiGate™ Next-Generation Firewalls, FortiSIEM™ Security Information and Event Manager

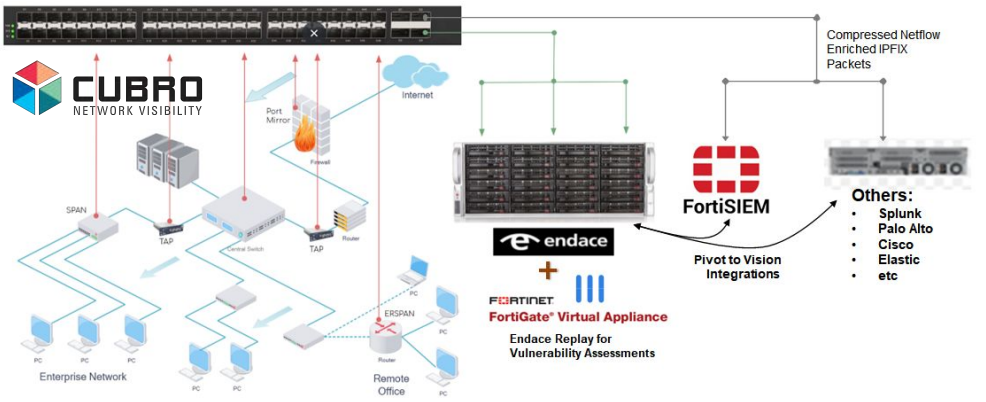
Solution Benefits:

- Streamlined investigation workflows from FortiSIEM with one-click access to full definitive packet evidence that accelerates investigations and enables accurate event reconstruction.
- Definitive evidence trail with an accurate record of all relevant packets related to any threat.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Zero-day threat risk validation with recorded network playback and threat analysis.

Security Incidence Response with Tamper-proof Evidence

Integrating FortiGate™ Next-Generation Firewalls, FortiSIEM™ and EndaceProbe Network History provides security threat detection, correlation, automated response, and remediation in a single, scalable solution. The solution defends against even the toughest threats by giving the entire SOC team access to rich, contextual, network evidence for fast and accurate decisions.

Fortinet's security-driven networking strategy tightly integrates an organization's network infrastructure and security architecture, enabling the network to evolve and grow without compromising security operations. FortiGate NGFWs deliver industry-leading enterprise security for any edge, at any scale, with full visibility and threat protection. FortiSIEM brings together visibility, correlation, automated response, and remediation in a single, scalable solution.



EndaceProbe™ Analytics Platforms capture, index and store network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. This recorded Network History provides the definitive evidence that helps the SecOps and NetOps teams to quickly and accurately investigate and respond to security threats and performance issues.

Cubro is a leading manufacturer and global supplier of IT network visibility products for Service Providers and Enterprise networks. Our product range includes Network TAPs and Advanced Network Packet Brokers that ensure the joint solution receives the network packet or flow data needed to perform the security function.

Why Use Cubro TAPs and Packet Brokers with Endace and Fortinet Solutions

Technically elegant solutions that provide **the best 'features to price' ratio**

Unique, advanced and standard, high performance product capabilities

Solutions have **low cost of entry, are easy to budget for, implement, expand and operate**

Easy to do business with - Cubro commercial and technical flexibility

World class technical support delivered from a local time zone

Widely deployed and proven products, technology and support

Cubro does NOT make or sell security solutions to compete with its technology partners

Brings the power of diverse security tool platforms to SDNs and the latest **cloud technologies:**

- Identifies overlays independent of host IPs
- Visibility into traffic from overlapping and duplicate IP or MAC address from different network tenants.

Fast, Accurate Security Investigation and Threat Hunting

The full Network History recorded by EndaceProbes is integrated into Fortinet users' workflows using the Pivot-To Vision™ function of the EndaceProbe API.

This integration lets security analysts pivot from security events detected by Fortinet directly to the EndaceVision™ investigation tool, to analyze the related network packet data, down to microsecond-level detail. The analyst can dissect, review and extract relevant traffic from within petabytes of Network History that has been recorded on EndaceProbes deployed on the network.

Zero-day threat risk validation with recorded network playback and threat analysis.

A zero-day threat is a computer-software vulnerability previously unknown to those who should be interested in its mitigation, like the vendor of the target software. Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers or a network.

A recent high impact example: In December 2021, Amazon Web Services, Microsoft, Cisco, Google Cloud, and IBM were among the major tech players affected by the Log4j vulnerability in an open-source logging library. The US Cybersecurity and Infrastructure Security Agency director described the flaw as, "one of the most serious I've seen in my entire career, if not the most serious."

When such events happen (widely reported, or not) company executives want to know: "Have we been affected?"

The EndaceProbe's Application Dock™ hosting capability extends security and performance monitoring by allowing third party analytics applications – including FortiGate Virtual NGFW - to be hosted on the open EndaceProbe platform. Hosted tools can analyze and inspect recorded traffic in real-time at full line-rate or analyze recorded Network History for back-in-time investigations.

In this way, a FortiGate firewall, newly updated with the latest threat signatures can analyze the impact of the zero-day threat and identify the affected systems or data.

These solutions depend on Cubro's Network TAPs and Packet Brokers to deliver the packet and flow data