SOLUTION BRIEF

Accelerate incident response and simplify network architecture with Niagara Networks and Endace Always-on Full packet capture.

The Problem

SecOps and NetOps teams need full visibility across the entire network to effectively manage performance and reliability and protect against security threats. But the complexity and dynamic nature of today's networks makes it difficult to eliminate blind spots and vulnerabilities in large, high-speed enterprise networks, potentially resulting in severe impacts to productivity and security.

Investigating and resolving performance, reliability and security issues across complex networks requires complete visibility into network traffic. Teams need access to data from across the entire network - on-prem, cloud and IT/OT - and often require days, weeks or months of recorded data to accurately reconstruct historical issues.

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 and decryption of network traffic so performance and security solutions have access to the most important data
- Integrates with always-on, full-packet capture to ensure all evidence is available
- Stores a definitive evidence trail with an accurate record of all relevant packets
- Provides deep lookback to enable accurate reconstruction, investigation and resolution of historical issues.

The Solution

By combining Niagara Network's visibility solutions with Endace's scalable, always-on, full packet capture, organizations gain unparalleled visibility into network activity and can secure the evidence analysts need to quickly and effectively identify, investigate and remediate network performance and security issues.

Niagara Networks provides a complete network visibility toolkit with an advanced visibility adaptation layer including TAPs, bypass switches, advanced network packet brokers and a unified management layer. This toolkit enables NetOps and SecOps teams to easily and efficiently manage multiple tools, enabling scale and flexibility while reducing operational expense and downtime.

Benefits

- Eliminate blind spots across physical, virtual and cloud networks to increase the overall 360 degree security posture
- Ultra-high resolution view of traffic intelligence - including TLS 1.3 encrypted data flows
- Scalable traffic optimization supports terabytes of aggregation capacity, filtering, deduplication, allowing traffic to be directed to where it's needed in the right format
- Streamlined investigation workflows from other tools your SecOps or NetOps teams use
- 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.

EndaceProbes capture, index and store 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. This enables organizations to extend their network and security monitoring capability by deploying instances of virtual applications anywhere they have EndaceProbes deployed. Hosted applications from partners including Cisco, Darktrace, Palo Alto Networks, Fortinet and many others can analyze real-time traffic at full line-rate for real-time detection or analyze recorded full packet data for powerful forensic investigation.

By connecting Niagara Networks Advanced Packet Brokers to EndaceProbe™ Analytics Platforms, traffic on different segments of the network can be easily aggregated, filtered, deduplicated, decrypted, and delivered to EndaceProbes for recording, inspection, and analysis.

SecOps or NetOps analysts can drill down - with full context surrounding alerts, threat indicators or performance issues - to analyze related full packet data in EndaceVision. EndaceVision lets them find, dissect, review and extract the relevant traffic in seconds from weeks or months of full-packet data recorded on the network, dramatically reducing investigation times and accelerating response.

Conclusion

Combining Niagara Networks visibility solutions with the EndaceProbe's full packet capture delivers definitive evidence that gives SecOps and NetOps teams the time and accurate forensic data they need to investigate and resolve even the most complex investigations across both physical and cloud environments.

Decryption of traffic before it is recorded gives SecOps teams visibility into threats that might otherwise be hidden in encrypted traffic. Additionally, by hosting third-party analytics tools in the EndaceProbe's Application Dock hosting environment, customers can extend their monitoring coverage without additional hardware deployments.

How it works

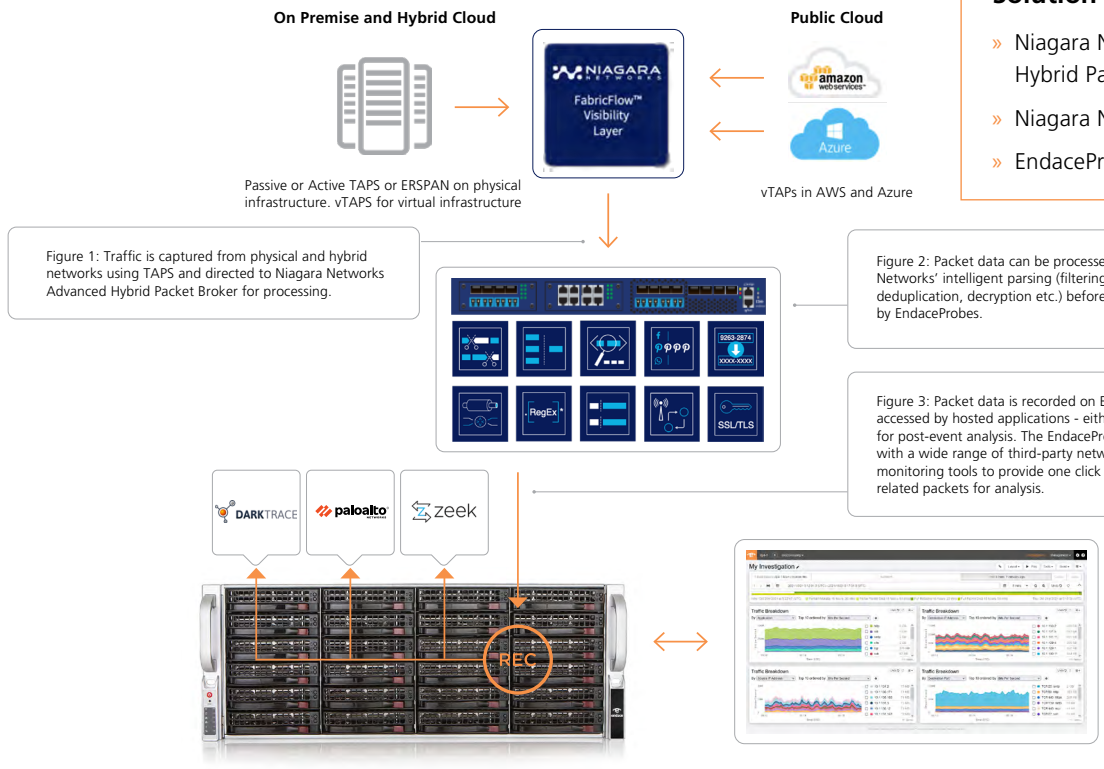

Figure 1: Traffic is captured from physical and hybrid networks using TAPS and directed to Niagara Networks Advanced Hybrid Packet Broker for processing.

Figure 2: Packet data can be processed using Niagara Networks' intelligent parsing (filtering, replicating, deduplication, decryption etc.) before being recorded by EndaceProbes.

Figure 3: Packet data is recorded on EndaceProbes where it can be accessed by hosted applications - either in real-time or replayed for post-event analysis. The EndaceProbe's API enables integration with a wide range of third-party network security and performance monitoring tools to provide one click drill-down from alerts to related packets for analysis.

Solution Components

- Niagara Networks Advanced Hybrid Packet Broker
- Niagara Networks TAPs
- EndaceProbe Analytics Platform