SOLUTION BRIEF

endace
Record. Respond.

Combine Garland Network TAPs and Packet Brokers with Endace Always-on Packet Capture for Fast, Accurate Resolution of Network Security and Performance Issues.

GARLAND TECHNOLOGY
See every bit, byte, and packet®

The Problem

For both NetOps and SecOps teams the complexity of modern networks presents serious challenges to adequately protecting against cyberthreats and investigating and resolving network security and performance issues. With networks spread across physical, virtual and cloud infrastructures, and running at increasingly high speeds, gaining full visibility across the entire network is both more difficult and more necessary than ever. Teams require not just real-time access to packet-level data but also access to historical data so they can quickly reconstruct, analyze and understand the full context of security and performance issues to enable fast, effective remediation.

Organizations need a solution that:

- Provides complete packet-level visibility to network traffic across the entire network infrastructure, to ensure NetOps and SecOps teams have access to the definitive evidence they need to analyze and respond to issues quickly and effectively.
- Provides the ability to search and drill down into historical, packet-level data to enable analysts to accurately reconstruct and investigate issues
- Provides optimized, load-balanced packet-level data for tool consumption
- Reduces costs by providing a combined tool environment running on the same hardware

The Solution

Combining Garland Network TAPs and Packet Brokers with the Always-on, full packet capture provided by the EndaceProbe™ Analytics Platform gives SecOps and NetOps teams access to a complete and accurate record of network traffic integrated that can be integrated directly into their preferred analysis tools. This puts definitive forensic evidence at analysts' fingertips for fast, accurate incident investigation and response.

Garland Technology's high-speed network TAPs deliver 100% raw packet data to Garland Technology's PacketMAX™ network packet broker, enabling advanced aggregation, filtering, and load-balancing.

For customers with virtual and hybrid networks, the Garland Technology Virtual TAP (GTvTAP) is a software-

Benefits

- 360° visibility with complete packet-level history across physical, virtual, and cloud networks.
- Optimized delivery of network telemetry to network security and performance monitoring tools
- Reliable traffic aggregation, load balancing, and filtering with full control over traffic behavior and flexibility for aggregation and regeneration
- Streamlined investigation workflows with one-click access to full definitive packet evidence to accelerate investigation and remediation and enable accurate reconstruction of events.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- The ability to deploy virtualized instances of tools across your environment for fast, efficient and cost-effective tool deployment.
- Definitive evidence trail with an accurate record of all relevant packets.
- High-availability with failover ensures EndaceProbe stacks stay operational when an EndaceProbe is under maintenance.

based TAP that mirrors or copies packets, encapsulates the packets using VxLAN, and sends the copies to an out-of-band virtual sensor, allowing EndaceProbes and other monitoring solutions to perform as promised in cloud environments. This provides tamper-proof network history from any part of your environment, including cloud-native applications and workloads, as well as on-prem infrastructure.

Load balanced traffic is delivered to EndaceProbes where the traffic is indexed and recorded ensuring teams have access to the relevant packet data for back-in-time investigation. Traffic can be analyzed in real-time and also replayed to monitoring tools to provide powerful back-in-time analytics – for example to check possible historical exposure to a new Zero Day threat.

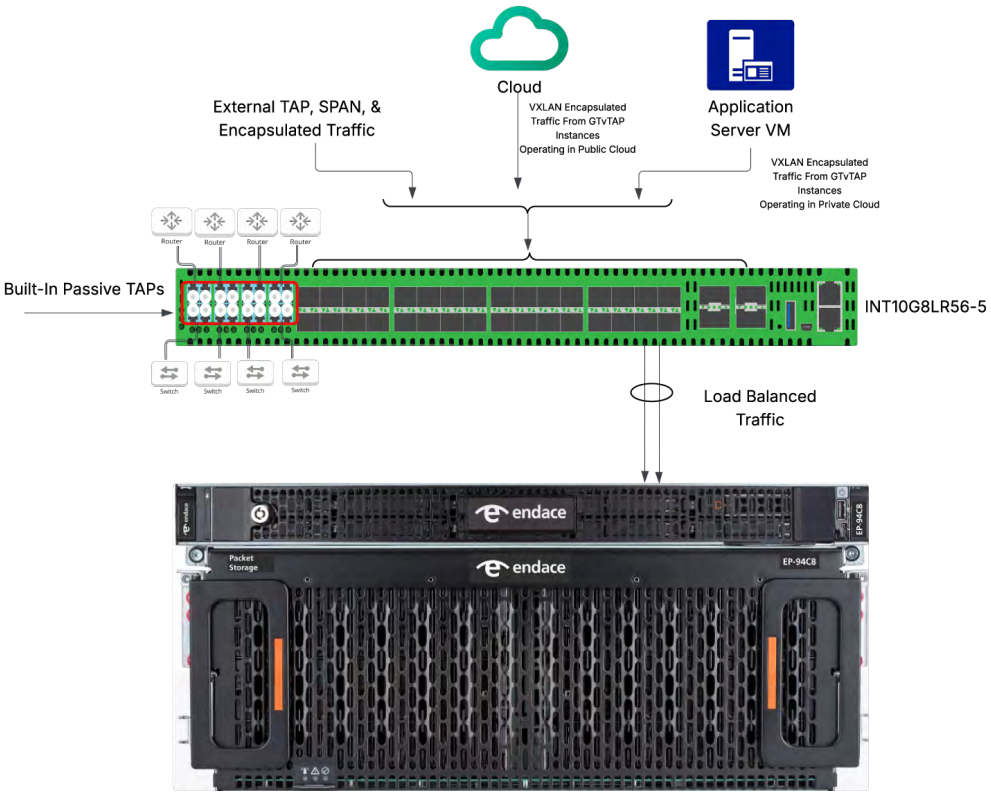
SecOps and NetOps analysts can drill down from alarm or threat indicators to the related network packet data in EndaceVision™ with a single click using the IP address and time range of the trigger event. EndaceVision lets them dissect, review and extract relevant traffic from within petabytes of recorded packet data quiclkly. Pivoting directly to the related packets with a single click lets analysts rapidly establish the root cause of issues, dramatically reducing the resolution time for resolving critical incidents and minimizing the risk of security threats escalating.

Deploying virtualized tools in the EndaceProbe's Application Dock hosting environment, lets customers extend their monitoring coverage without additional hardware deployments, leveraging existing EndaceProbe hardware to deploy new or upgraded traffic monitoring and analysis capability.

Conclusion

Integrating Garland Technology's TAPs and Network Packet Brokers with EndaceProbes eliminates without blind-spots across the entire hybrid network environment. Teams can investigate threats and performance issues using definitive evidence that enables them to respond to incidents more quickly and effectively.

How it works



Solution Components

- Garland Technology Network TAPs and Packet Brokers
- EndaceProbes