Garland Technology and Endace

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Ensure complete packet capture to investigate network traffic.

When employing secured business operations, network engineers must be well equipped with the right tools to prevail against looming network threats. Designing your infrastructure using enabling components to gain a foundation of visibility will ensure optimal performance from your tools.

To protect the network and accurately detect cyberthreats and performance issues, network security and monitoring tools need complete packet-level visibility to ensure they have access to all the traffic they need to analyze. SecOps and NetOps analysts also need to be able to look back in time and drill down into historical network traffic so they can quickly and accurately investigate network performance issues or security threats.

How Garland Technology and Endace Work Together

1. Garland Technology's high-speed network TAPs deliver 100% raw packet data for full network visibility.
2. The TAPs deliver packet-level data to Garland Technology's PacketMAX™ network packet broker, enabling advanced aggregation, filtering, and load-balancing.
3. Load balanced traffic is delivered to EndaceProbe™ Analytics Platforms where the traffic is indexed and recorded. Traffic can also be analyzed in real-time by third-party analytics applications running in the EndaceProbe's Application Dock™ hosting environment.

Expanding Your Network Architecture

Anywhere EndaceProbes are deployed, customers can extend their network and security monitoring capability by deploying a wide range of third-party commercial or open-source analytics applications in Application Dock.

Hosting solutions such as Palo Alto VM Series Firewalls, Cisco Firepower and Stealthwatch, AI-based security solutions from Darktrace or Bluvector or open-source tools like SNORT or Zeek on EndaceProbes enables customers to extend capability and adapt to changing needs quickly without having to deploy new hardware. These tools can analyze and inspect recorded traffic in real-time at full line-rate or analyze recorded network history for back-in-time investigation.

PRODUCTS

Garland Technology Network TAPs and Packet Brokers

Garland Prism

EndaceProbes

BENEFITS

- 360° visibility with complete packet-level history across physical, virtual, and cloud networks.
- Optimization of network security and monitoring tools
- Reliable traffic aggregation, load balancing, and filtering with full control over traffic behavior and flexibility for aggregation and regeneration
- Streamlined investigation workflows from the tools used by your SecOps or NetOps teams, provides one-click access to full definitive packet evidence that accelerates investigation and remediation and enables accurate reconstruction of events.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Leverage your always-on packet capture appliances to also 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.

Confidently Accelerate Investigations

Garland Technology delivers network traffic, at full line rate, to EndaceProbes where it is continually indexed and recorded (with zero packet loss) and stored for back-in-time investigations using Playback™. Operations teams can leverage workflow integrations that use the EndaceProbe's powerful Pivot-To Vision™ API. Pivot-To-Vision lets security analysts pivot from alerts in SIEMs - like Splunk, QRadar, ArcSight and Elastic - or monitoring tools – such as Plixer, Darktrace, BluVector, and more - into EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History.

END_fp_end_garland_1.0_0221

Network and Security Operations Benefits

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 the relevant traffic from the petabytes of recorded Network History. It supports analysis to microsecond level detail with views filtered by Application, IP, Protocol, Top Talkers, and many other parameters, providing rapid insights and enabling accurate conclusions.

Pivoting directly to the related packets with a single click lets analysts rapidly establish the root cause of issues during threat hunting or when investigating security or performance issues. This lets them respond quickly, dramatically reducing the resolution time for resolving critical incidents and minimizing the risk of security threats escalating.

Gain Visibility Across your Hybrid Cloud Infrastructure

Networks are increasingly complex, with components deployed both on-premise and in the cloud (public or private) environments to give you the elasticity and agility needed for your business. With the complex, dynamic nature of your network, it is more critical than ever that monitoring and security tools continue to have visibility across both the physical and cloud environments - with no blind-spots.

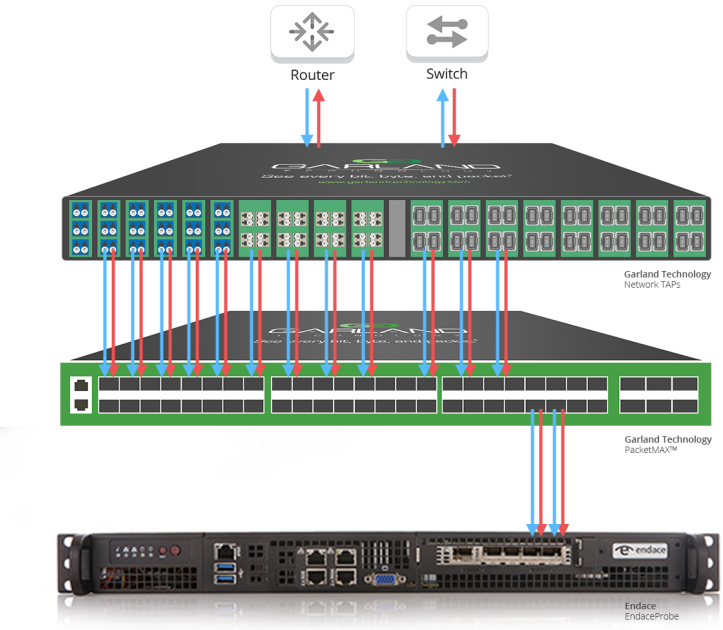
Prism, Garland Technology's virtual TAP, provides comprehensive insights from any cloud provider or on-premise deployment. With a centralized cloud management control panel, cloud traffic is forwarded to the EndaceProbes and advanced tools. This provides tamper-proof network history from any part of your environment, including cloud-native applications and workloads, as well as core infrastructure network traffic.

Conclusion

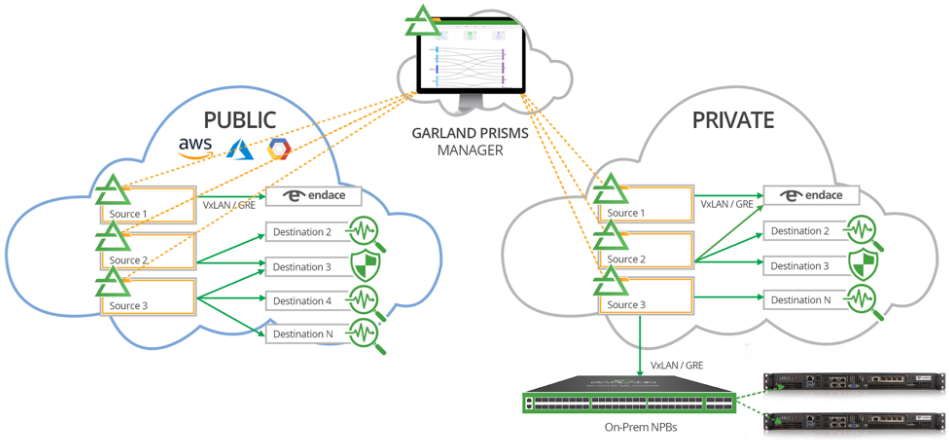
Integrating Garland Technology's TAPs and Network Packet Brokers with EndaceProbes lets security teams respond to alerts faster and investigate threats with confidence across both their physical and cloud environments without blind-spots. Deploying virtualized tools in the EndaceProbe's Application Dock 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.

Example Deployment Architecture

On-premise deployment



Hybrid Cloud Environment



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

For further information, email: info@endace.com

END_fp_end_garland_1.0_0221