Empowering Your Infrastructure with Deep Packet Inspection

A Joint Solution from OORIGIN and Garland Technology

Network Clarity with Full Packet Capture by Inspecting IP Traffic and Data Flows

When securing data traffic, empowering your infrastructure for deep packet inspection becomes a central priority to build a secure environment. The network is the lifeline of the data center. Data processing deep packet inspection is an integral part to inspect the detail of the data being sent over the network. In order to acquire packets to enable network management and DPI, network TAPs are required to feed the system.

OORIGIN by Orsec Technologies SAS and Garland Technology have partnered to provide a high capacity solution. Using Garland Network TAPs to feed Orsec Network Monitoring Software, for a complete 100% visibility of your network traffic to check for malicious packets, and block, re-route, or log data accordingly. Together, the two are deployed in a range of applications at the enterprise level.

End-To-End Visibility and Network Integrity
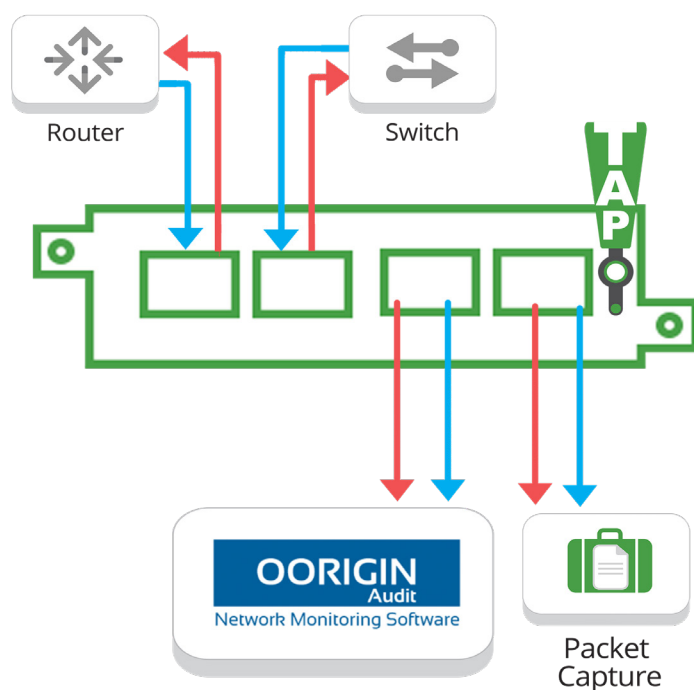
Garland Technology's Network TAP is used to gain visibility into the network, delivering packets to Orsec's forensic DPI tool. The routed traffic is classified into IP traffic using 2900 signatures of protocol and layer 7 applications to generate logs for meaningful insights. This streamed process between Garland Network TAP and Orsec's DPI tool performs inline decoding that allows visibility into every transaction on the network. The IPS traffic with IP Geolocation and integrated Cyber Threat Intelligence database helps to easily evaluate and optimize inline devices by determining final latency.

Live Wire Data Inspection with Forensic Monitoring

Deep packet inspection is necessary to gauge and monitor the performance of network traffic. Using live wire data, Garland Technology and Orsec's end-to-end visibility solution drives traffic from the network TAPs to Garland's PacketMax Advanced Aggregators to aggregate and load balance the data. Once delivered to Orsec's forensic monitoring appliance, the tool will address IP threats from cyberattacks, spyware, and viruses in the network by eliminating blind spots. This scalable solution enables completely accurate visibility to produce reports that analyze anonymizing services, like proxies, that may represent a risk for the network.
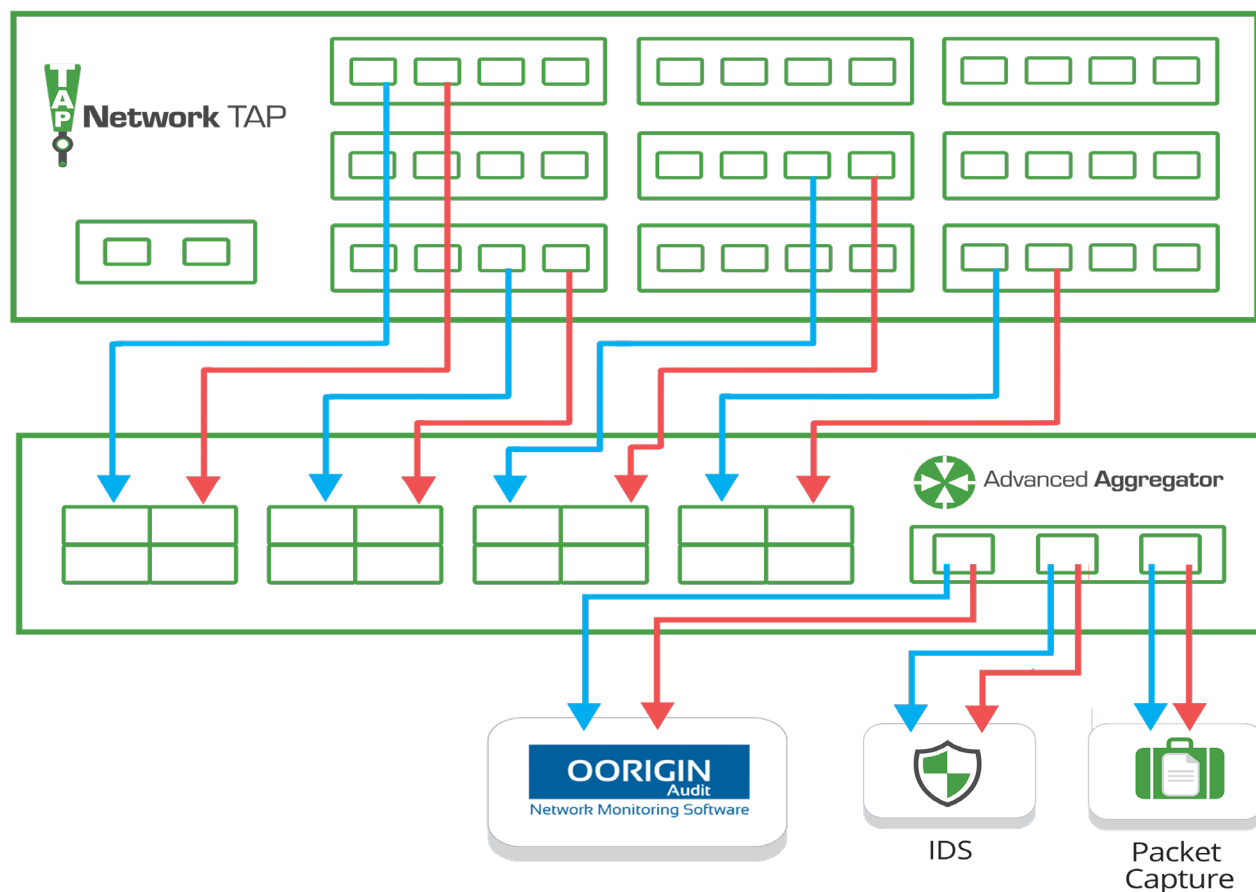
Garland Technology Network TAPs and Packet Brokers

Garland Technology provides a full platform of network access products including a range of network TAPs and Network Packet Broker devices, supporting the entire wire spectrum from 10/100M copper to 1G/10G/40G/100G.

Key Capabilities

- **Complete Network Visibility** by passing all live wire data

- **Ensure No Dropped Packets** for out-of-band tools

- **Quality standard**, all TAPs are tested with live network data and validated

- **100% failsafe packet capture** – built-in failsafe and/or heartbeat technology.

- **Reliable traffic aggregation, load balancing, and filtering** – full control over traffic behavior and flexibility for aggregation and regeneration.

OORIGIN Network Monitoring Software

OORIGIN is a passive network monitoring software powered by advanced DPI technology. OORIGIN inspects your IPv4 traffic and classifies it into flows, describing the protocols, application events, and associated metadata.

Key Capabilities

- **Device inventory -** Analyze devices communicating on your network and discover shadow IT equipment

- **Device profiling** - Server, NAS, computer, printer, router, IoT, industrial, network activity profiling

- **Application profiling** - Study a specific application to detect potential security issue or data leak

- **IT Policy enforcement** - To verify end-user's adherence to IT policies (ex: gaming, mine bitcoins)

- **Data Retention -** Store the network activity logs for future investigations

- **Regulatory Compliance** GDPR, ISO27001, PCI security audits

- **IT Infrastructure** - Improve your IT infrastructure by getting better understanding on how it is used

- **Cyber investigation -** Investigate cyber incident with the level of details of a full capture log

GARLAND
T E C H N O L O G Y
See every bit, byte, and packet®

OORIGIN
By Orsec Technologies SAS