

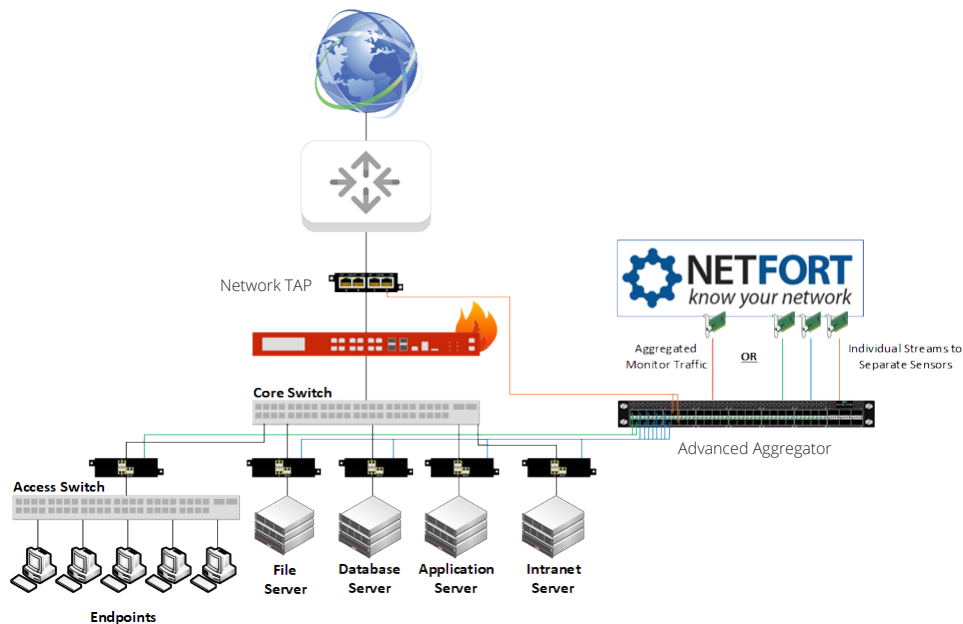
# How to get Comprehensive Internal Visibility on any Network

A joint solution from NetFort and Garland Technology

## 100% Live Wire Data Enables Comprehensive, Scalable Network Traffic Analysis and Rich Actionable Metadata for Network Security and Operations

In an ever growing network security landscape, the Education, Government and Financial sectors have to be able to monitor, troubleshoot and report on everyday network and user activities. Whether it's for bandwidth issues, suspicious traffic, unusual usage, policy violations, or possible internal security threats, continuous internal visibility is imperative.

NetFort and Garland Technology have partnered to offer an integrated solution using Garland Technology's high performance network test access points (TAPs) and aggregators, that deliver a complete copy of network traffic to NetFort's network traffic analyser providing unique levels of visibility into internal user and device activity.



Instead of using a SPAN or Mirror port on a switch, Garland Technology's Network TAPs can be strategically placed to capture data traveling to key areas in the network. Each TAP will produce a monitor link containing an exact copy of the data traversing the cable. If multiple TAPs are placed around the network, these monitor links can be collected together using Garland's Advanced Aggregator. Once aggregated, the tapped traffic can be sent to a LANGuardian Sensor as a single stream of data or broken into streams from certain sections of the network to individual sensors.

# Garland Technology

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

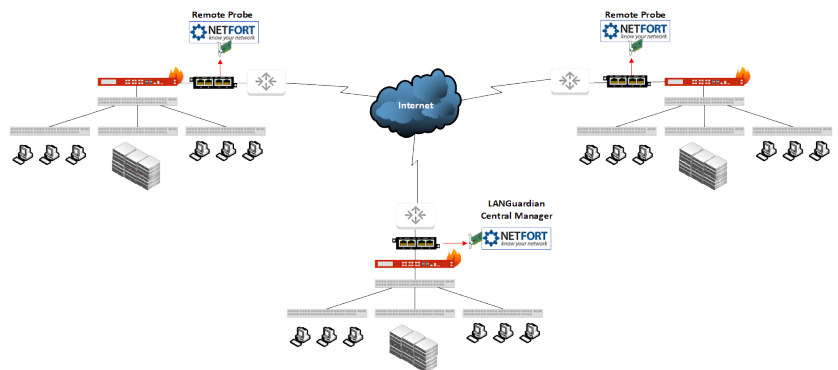
## Key Capabilities

- **Complete Network Visibility** by passing all live wire data
- **Ensure No Dropped Packets** for out-of-band tools
- **100%, failsafe packet capture** – all Network TAPs are tested and validated and have 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.

## Use Case

### Scalability with Remote Deployments

In situations where a company has multiple locations, Remote LANGuardian Probes can be deployed at remote sites and report back to the Central Manager at the main location. TAPs can be used to feed the probes at both the remote locations and the central location.



# NetFort LANGuardian

LANGuardian ensures organisations of all sizes have internal traffic visibility across their virtual, physical and cloud networks. LANGuardian provides real time and historical metadata, rich detail and context about what's happening on the wire. It is the ideal single point of reference for network traffic, user and security monitoring and the first stop for troubleshooting any issues.

## Key Capabilities

- **Internal visibility in minutes** – Easy to Implement, download and deploy on standard server hardware or VMware. Connect to a Garland TAP and get visibility anywhere in minutes.
- **Search by user name** – Search all traffic, events, internal activity including accesses to data, file shares, SQL databases and Internet by IP address and user name.
- **More detail than NetFlow** - NetFort's network traffic analysis engine transforms raw traffic into rich application centric metadata. More drill down and detail than flow technologies such as NetFlow without the complexity and costs associated with full packet capture.
- **Real-Time and Historical context** – Go back, get instant access to all the traffic data and context required to understand exactly what happened before and after the incident.

## About Netfort

NetFort provides network traffic and security monitoring software for virtual and physical networks. NetFort's flagship product, LANGuardian, is unique in the marketplace thanks to the rich metadata generated by its powerful network traffic analysis engine. LANGuardian continually monitors and analyzes the traffic trail left on any network by devices/users and decodes key applications including Internet, SMB, SQL, DNS, SMTP and DHCP. [www.netfort.com](http://www.netfort.com)



Have Questions? [sales@garlandtechnology.com](mailto:sales@garlandtechnology.com) | +1 716.242.8500 | [garlandtechnology.com](http://garlandtechnology.com)

Garland Technology is an industry leader delivering network products and solutions for enterprises, service providers, and government agencies worldwide. Since 2010, Garland Technology has developed the industry's most reliable test access points (TAPs), enabling data centers to address IT challenges and gain complete network visibility. For more information, or learn more about the inventor of the first bypass TAP, visit [GarlandTechnology.com](http://GarlandTechnology.com) or [@GarlandTech](https://twitter.com/GarlandTech).

