CASE STUDY

GARLAND TECHNOLOGY
See every bit, byte, and packet.™

Security: Healthcare

How to Gain Full Visibility During an Instant Response Data Breach

Cyber Defense Group, an incident response firm needed to gain visibility to contain a breach on a large healthcare facility's network. With a complicated network environment stacked with legacy equipment, and staffed with basic onsite IT and an underperforming MSSP, the facility was overwhelmed.

The network seemed to work great when there was nothing wrong, but issues were quickly exposed during the attacks in this scenario. Once they were under attack, it became apparent that the network was not set up properly with zero visibility. The existing switches didn't have the proper firmware updates, they weren't configured correctly and had ingress / egress set up issues.

Challenge: The first challenge was gaining visibility to monitor the network traffic: understand where the attackers were coming from, where they might be touching internally, and how to stop them.

> **“*We're under attack and every minute that we don't have visibility, is another minute that bad guys are exfiltrating sensitive data.***
>
> *- Lou Rabon, Founder/CEO, Cyber Defense Group*

The second challenge was finding the right vendor to provide that access and visibility. “Before we found Garland our options were limited. It's either we go to a huge provider like Gigamon, which is super expensive, and doesn't give you a custom solution. Or the other end of the spectrum would be buying a 1G consumer grade mirror on Amazon and that wasn't going to solve our problem.”

Goal: Quickly gain visibility, to contain a breach on a large healthcare facility's network.

Solution: Out-of-band security and monitoring tools analyze packet data from the production network to provide insights or alerts for SecOps and NetOps teams to properly respond. These packets are delivered to solutions by either Network TAPs or SPAN ports both mirror traffic from ports to out-of-band solutions.

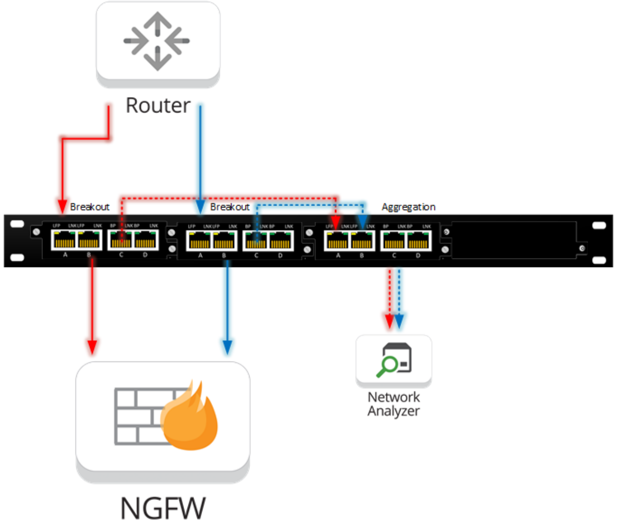

Diagram: Breakout' TAPs and one Bypass TAP, in aggregation mode

Cyber Defense Group utilized two Garland Technology 'Breakout' TAPs and one Bypass TAP, in aggregation mode to feed the proprietary tools they use for intrusion detection system (IDS), security monitoring, NGFW and log management.

> ***We were able to get the visiblity we needed quickly. That allowed us to do what we needed to find the bad guys and kick them out.***
>
> *- Lou Rabon, Founder/CEO, Cyber Defense Group*

TAP 'Breakout' mode sends each side of traffic to separate monitoring ports. Ensuring that no packet is lost to high-priority monitoring tools. Aggregation mode merges traffic streams into one monitoring port to reduce appliance costs, often used in combination with filtering taps, ie: filter, aggregate data streams.

Benefits:

- After installing Garland's network TAPs, CDG easily diagnosed and resolved the breach
- Not knowing what they needed, the Garland team helped design the deployment to quickly resolve the issue
- Improve risk assessment
- Enable security technology upgrades

Looking to add visibility and improve threat detection, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it's what we love to do.