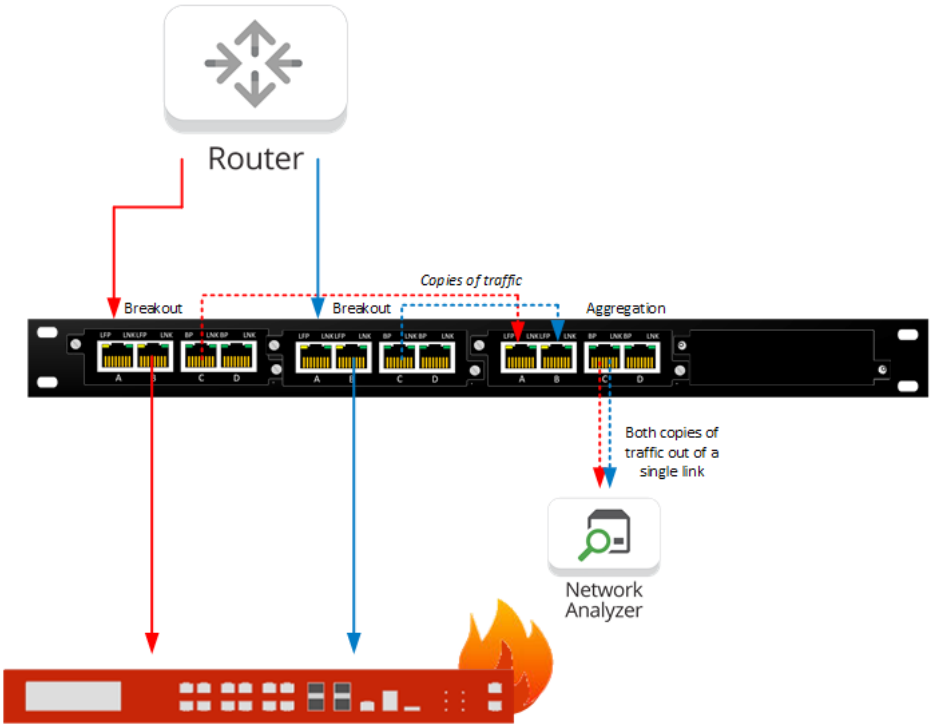
Security: Healthcare

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.

Pain point: The network seem to function good when there is nothing wrong but issues were quickly exposed during the attack. Once under attack, it became apparent that the network was not set up properly, the existing switches didn't have the proper firmware, they weren't configured correctly and had ingress / egress set up issues. This proved diagnosing the problems with low network visibility difficult.

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



Solution: Cyber Defense Group accomplished this by utilizing two Garland Technology Copper Network TAPs in 'Breakout' mode and one EdgeSafe™: Bypass Network TAP, in aggregation mode to feed proprietary tools they use for full packet capture in the cloud, intrusion detection (IDS), enterprise security monitoring, NGFW and log management.

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

"When I found Garland, I got a network expert on the phone and they configured a custom solution for us. Really from the beginning, from sales to the solution, to support. I can't say enough good things."

-Lou Rabon, Founder / CEO, Cyber Defense Group

Value:

- After installing Garland's 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.