



Network TAPs and Network-based Threat Detection

High Performance Network Detection

PROBLEM

Keeping an enterprise network and associated assets secure is an immense responsibility. Organizations large and small cannot properly deliver on their promise to stakeholders without a well-functioning and secure network infrastructure. At the same time, the pressures on cyber defenders to quickly assess and respond to threats such as attacks from ransomware and spyware, in real-time, is intense. Lack of visibility into segments of the network or a single ignored warning can turn a demanding day into a stressful scramble at best, and possibly even a serious breach.

SOLUTION

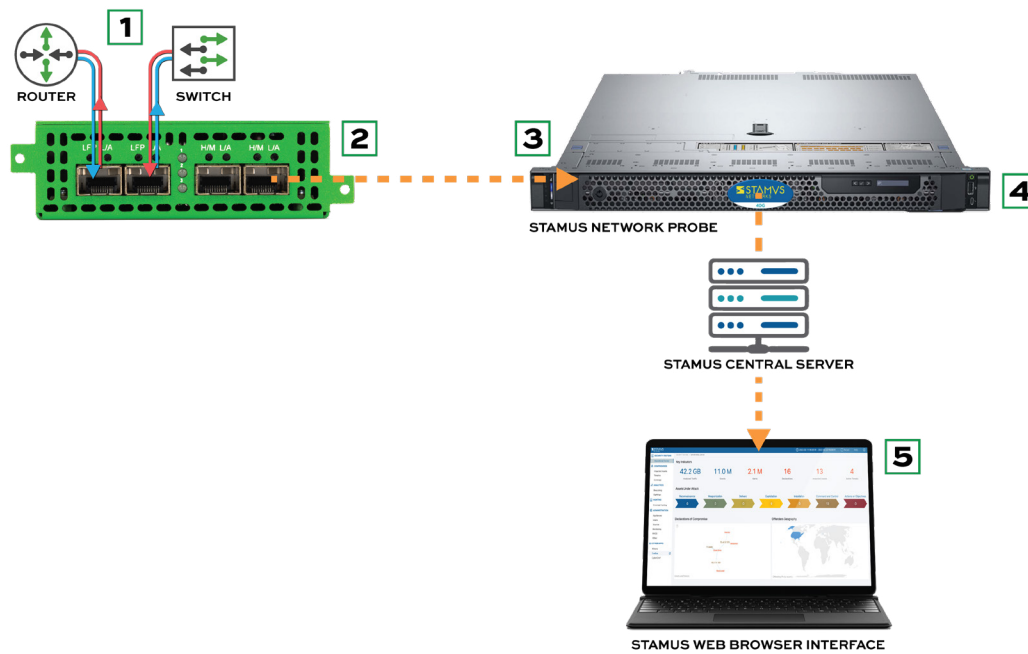
Effective enterprise network-based threat detection and response is possible with the Clear NDR™ from Stamus Networks. Clear NDR delivers broad-spectrum threat detection in an open system, providing defenders with response-ready and high-fidelity notifications from machine learning, stateful logic, and signatures.

To do so, Clear NDR inspects all network traffic from a Garland Technology Network TAP. Network TAPs are the most reliable way to ensure the Clear NDR has full visibility into all segments of the enterprise network. Garland's Network TAPs deliver copies of full duplex traffic from the network to the Clear NDR immediately upon installation. Clear NDR then helps SecOps and NetOps with automated detection, proactive threat hunting, incident investigation, and IT policy enforcement.

BENEFITS

The joint solution from Stamus Networks and Garland Technology ensures threat detection and insights are prompt and turnkey. This solution offers complete visibility of enterprise network traffic, detecting threats that other methods miss. This complete visibility into network activity, coupled with high-fidelity detection and automated event triage, allows security operations personnel to focus on serious and imminent threats. Also, this visibility with over 4,000 unique elements of network metadata allows network operations teams to effectively maintain and troubleshoot the network.

An added benefit of connecting the Clear NDR using Network TAPs is the added peace of mind that Network TAPs will not be an added vulnerability in the network. Network TAPs cannot be hacked because they do not have an IP address or MAC address. Also, because Network TAPs do not drop packets, Clear NDR is guaranteed to receive all the network traffic needed to perform its job properly. Network TAPs will never oversubscribe Clear NDR or negatively affect network uptime.



HOW THE SOLUTION WORKS

1. Network TAPs from Garland Technology connect to the on-premise IT network by installing between two network devices.
2. One or more Clear NDR Probes connect to the network TAPs.
3. Network TAPs copy full-duplex traffic and send the copies to the out-of-band Stamus Network Probes.
4. The Clear NDR Probes, which are based on the Suricata open-source network security engine, receive copies of the traffic and perform real-time threat detection, enrich the resulting events with extensive metadata, and capture network protocol transactions.
5. Clear NDR Probes then feed the Clear NDR Central Server for additional threat detection and advanced analytics along with a guided threat hunting interface. Users access the entire system via web browser.

About Stamus Networks

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

About Garland Technology

Garland Technology is a USA-based manufacturer of network TAPs, network Packet Brokers, and Inline Bypass solutions. We engineer, manufacture, and support our hardware solutions in Richardson, Texas. Since 2011, we've been helping companies' network monitoring and security tools deliver on their promise of performance and protection because we reliably deliver all the data the tools need to shine. For help with projects large and small including installations, upgrades, and streamlines, or to learn more about the inventor of the first bypass technology, visit GarlandTechnology.com or [@garland-technology-llc](https://twitter.com/garland-technology-llc).



Have Questions?

sales@garlandtechnology.com | +1 716.242.8500
GarlandTechnology.com/stamus-networks

