

- LIGHTCYBER & NIAGARA NETWORKS PROVIDE TURN-KEY NETWORK VISIBILITY AND ATTACK DETECTION SECURITY SOLUTION -

Comprehensive Network Monitoring and Behavioral Attack Detection

LightCyber, a leader in Behavioral Attack Detection and Niagara Networks, a leader in Network Visibility and Uptime Solutions have partnered to ensure a comprehensive network security solution by providing behavior-based attack detection and access to all network traffic so there is full coverage across single and multi-network link deployments.

The joint LightCyber and Niagara Networks solution offers a cost-effective way to provide highly granular network visibility, cyber security, deep packet inspection, agentless endpoint monitoring, and behavioral analysis to detect sophisticated and evolving attacks in real time. Together, LightCyber and Niagara Networks ensure a plug-and-play passive monitoring solution that delivers industry leading network attack detection while ensuring network visibility and uptime, with intuitive and comprehensive user interface, reporting and alerts.

Challenge

Signature based security solutions are failing to keep up with the evolution of the increasingly sophisticated and ever-changing landscape of security threats. In addition, there are very few solutions that provide protection at the gateway, core networks, remote sites, and end points, often rendering de-centralized security solutions ineffective or insufficient.

A solution is required that can provide advanced detection in real time and can evolve with the security threat landscape and explosive growth of network bandwidth. This solution needs to ensure new and evolving attacks, including attacks that make no use of malware, are swiftly detected while ensuring visibility across all network nodes throughout network topologies.

Solution

Together, LightCyber and Niagara Networks provide a scalable solution that ensures Network Visibility into 1G and 10G Critical Network links and can provide access to the appropriate network traffic for identification of opportunistic infections, risky behavior and insider attacks, and advanced or targeted attacks.

The Network TAP ports of the Niagara 2804 connect to each side of one or multiple bi-directional 1G or 10G network links and transparently pass network traffic while ensuring network uptime in case of any power failure, link loss or software crash via fail-to-wire protection. The Packet Broker ports (which come in empty cage 1G/10G flexible SFP+ ports) provide the ability to load balance, aggregate, filter and/or mirror the tapped Network traffic to one or multiple LightCyber Magna Detectors.

SOLUTION BENEFIT SUMMARY

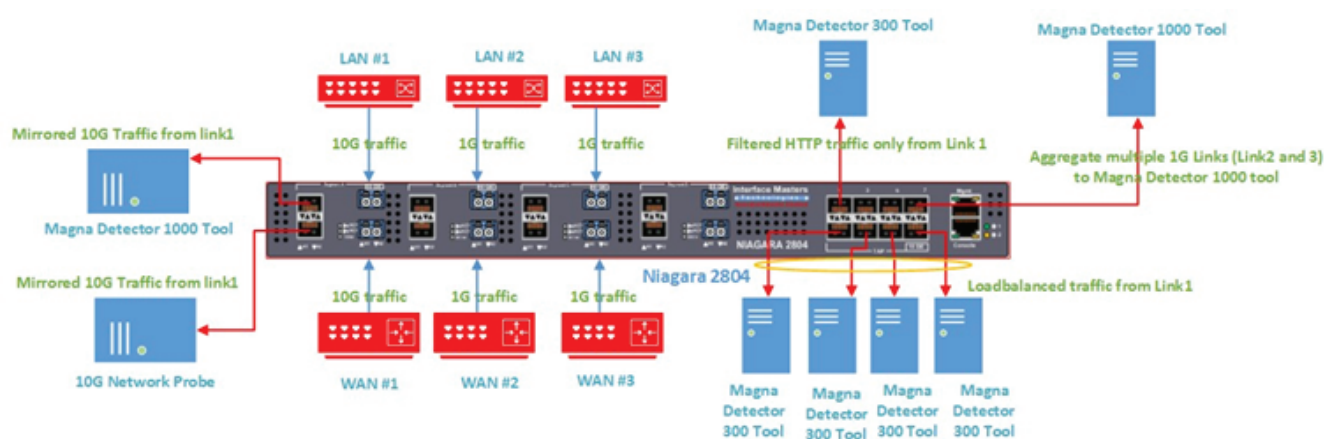
- Plug & Play, User friendly Web GUI/Management
- Scalable Enterprise Grade Visibility & Security Solution
- Ensures Comprehensive Network Access, Visibility and uptime
- Support for 10G & 1G Network TAP, Filtering, Mirroring, Aggregation, Load Balancing and Speed Conversion between Network Links & Monitoring/Security Tools
- Continuous Monitoring and Breach Detection
- Comprehensive Network Forensics
- Software based Sensors can be deployed on commodity hardware or in virtual environments
- Detection via Analytics, Signature, Behavioral and File Analysis
- Query and Visualize Network Traffic
- Network Analytics, Reporting and Alerting
- Cost-Effective Solution

Magna Detectors possess functions that provide proactive and intelligent attack detection including identification and remediation of command and control, reconnaissance, lateral movement, and data exfiltration. The integrated solution provides a seamless passive network monitoring and visibility solution tailored to safeguard enterprises, service providers, TELCOs, datacenters, governments and institutions.

Solution Applications

Common applications of the Niagara Networks Niagara 2804 and LightCyber Magna Detector solution are:

- Niagara 2804 provides session based loadbalancing and network speed conversion which enables 10G Network links to be monitored efficiently by Magna Detectors. With the Niagara 2804 in place, an end customer can simply connect 10G Network links into the Niagara 2804 and loadbalance the 10G feed to a series of Magna Detector appliances of any size, while maintaining session integrity
- Niagara 2804 provides ability to Filter 10G traffic based on IP, MAC, Port, Protocol, VLAN ID or create a user defined byte and then send only the traffic that is relevant to the Magna Detector for processing, enabling the Magna Detector to focus on the types of network traffic that pose a threat to the network and ignore the rest. An example would be to take in a 10G feed and filter out unneeded traffic such as server backup traffic, while sending only necessary traffic via a Niagara Packet Broker port to a port on a Magna Detector
- Niagara 2804 provides the capability to take in a 10G or 1G network feed and mirror that traffic to multiple Magna Detector systems to provide in in-depth, multi-layered analysis on the same critical network link
- Niagara 2804 can enable multiple 1G network links to be tapped and aggregated to a single larger Magna Detector appliance for analysis and monitoring. An example would be tapping the marketing, accounting, engineering and operations department 1G network links, collecting and aggregating the traffic via the Niagara 2804 and sending the traffic to a single Magna Detector.



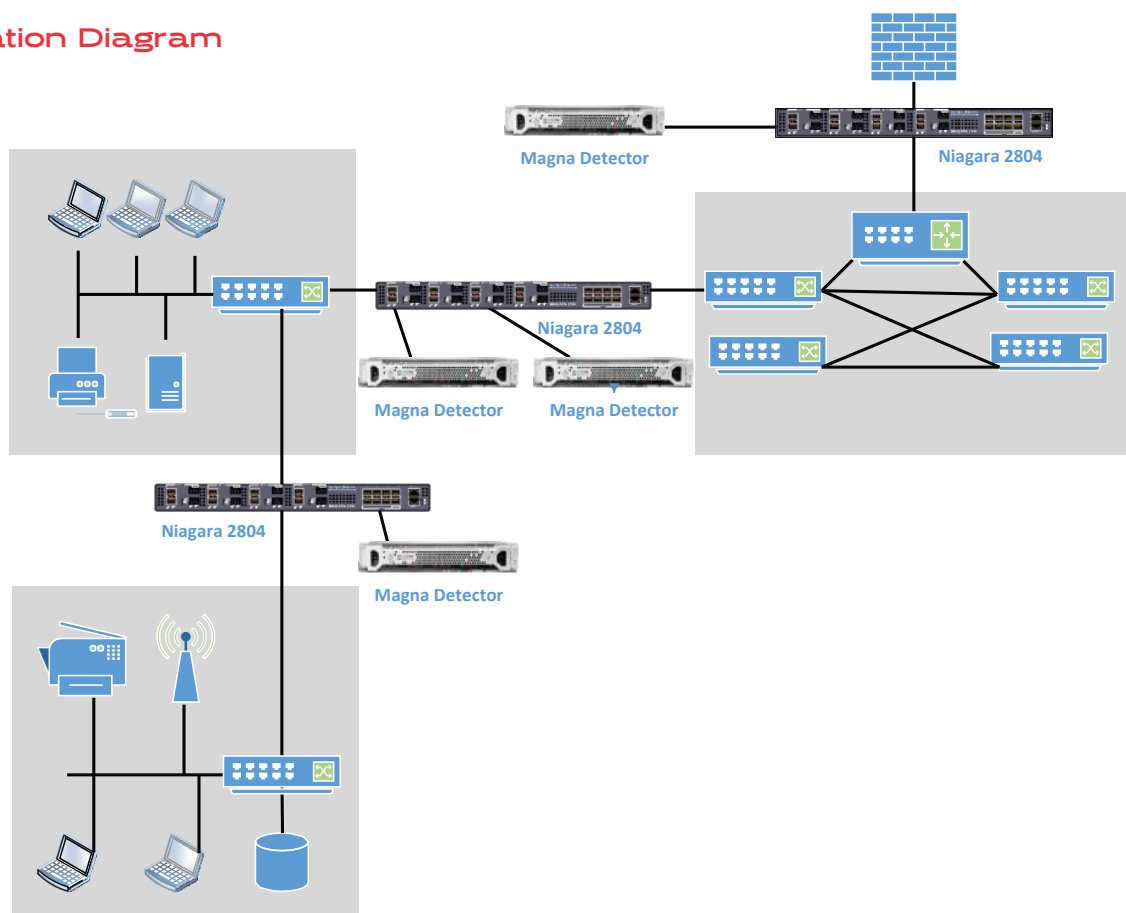
Application Diagram – Interface Masters Niagara 2804 and LightCyber Magna Detector Tools

Deployment Options

The Solution can be passively deployed at any strategic network point including:

- Core/BackBone
- Site to Site
- Edge
- Distribution
- Corporate Backhaul
- DataCenter/Central Office
- Access
- Remote Office
- DMZ

Application Diagram



Example Network Topology Diagram

About LightCyber

LightCyber is a leading provider of Behavioral Attack Detection solutions that provide accurate and efficient security visibility into attacks that have circumvented traditional security controls. The LightCyber Magna™ platform is the first security product to integrate user, network and endpoint context to provide security visibility into a range of attack activity. Founded in 2011 and led by world-class cyber security experts, the company's products have been successfully deployed by top-tier customers around the world in the financial, legal, telecom, government, media and technology sectors. For more information, please visit www.lightcyber.com

About Niagara Networks

Niagara Networks is a Network Visibility industry leader, with emphasis in 1/10/40/100 Gigabit systems including Network TAPs, External Bypass Switches, and Network Packet Brokers that integrate with monitoring systems, inline networking appliances, IPS, UTM, Load Balancing, WAN acceleration, and other mission-critical IT and security appliances. Formerly part of Interface Masters, a Silicon Valley based network solutions company, Niagara Networks recently spun off from Interface Masters to focus on its core competencies, and developed an independent company identity.

Niagara Networks offers the highest port-density systems, the most complete hybrid systems, and the highest quality and feature-rich Bypass Solutions in the market. Niagara's unique and modular designs, innovative next generation Network Visibility technology, including the 100 Gigabit-capable Network Packet Broker with hybrid functionality, and the ability to tailor systems to exact customer specifications, allow it to lead the industry with high quality, innovative products and exceptional service. For more information, please go to: www.niagaranetworks.com



USA	EMEA
+1 408 622 0354	+44 20 3514 2567
+1 408 213 7529	+1 408 213 7529
sales@niagaranetworks.com	emea@niagaranetworks.com
150 E. Brokaw Rd., San Jose, Ca 95112	

