Automated Mass Cyber Surveillance for Optical Networks

Global networks are facing unprecedented levels of targeted attacks and cyber threats. These threats are becoming more difficult to detect as attackers constantly adjust their tactics and techniques. Complicating matters, network bandwidth rates continue to rise exponentially as new data transport technologies emerge.

Nowhere is the cyber defense workforce more challenged than in the protection of the global optical network. Contrary to popular belief, optical networks, not satellites, are responsible for carrying over 99% of the global intercontinental traffic. These information highways represent an ideal location for detecting cyber-attacks and defending national security interests.

Unfortunately, network visibility solutions designed to detect criminal activity across thousands of fibers, each capable of carrying terabits of traffic, is a costly endeavor and one that many have compromised to meet CAPEX and OPEX budget constraints.

Solution: Scalable Access for 100% Visibility

Monitoring fiber networks at this scale requires significant levels of manual survey to enable access to targeted IP traffic and generate invaluable SIGINT. A viable solution must automate the process of continual network survey and reuse precious capital equipment.

NetQuest's OMX3200 replaces the need for lengthy manual labor diagnosing WAN protocols by offering automated network survey via zero-touch WAN auto-discovery. The OMX will extract targeted IP traffic carried over DWDM, Ethernet, OTN and legacy SDH networks and combine this with line-rate advanced packet processing and enriched IPFIX metadata generation.

Huber+Suhner Polatis provides dynamic high-capacity all-optical switching between large fiber networks and analysis tools, allowing large monitoring solutions to leverage costly tool ports across many fibers. Ultra-low optical insertion loss is critical for monitoring long-haul and regional networks where minimizing optical impairments is necessary for preserving signal characteristics and link margins.

- Rotate connection to fibers
- Record network survey info
- Generate enriched metadata
- Automate traffic intercept

NetQuest's Alpine Patrol software combines these 2 technologies to provide an automated application capable of scaling to meet the demands of international optical networks. The solution scans large fiber plants to track signaling contents by storing intelligent metadata so that critical surveillance can be enabled for individual fibers on demand. The solution dramatically reduces cost by removing the need for on-premise engineers and significantly reducing the required number of SIGINT tool ports.
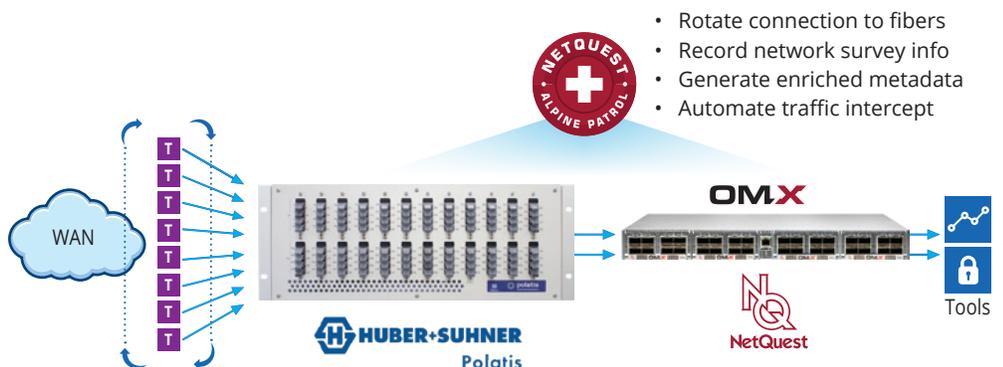
Who We Are

NetQuest is a trusted and longstanding supplier of high-performance Cyber Surveillance solutions to government agencies around the globe.

With the introduction of the OMX Optical Monitoring Exchange we have built upon our 30+ years of network monitoring experience and applied the indepth cyber knowledge we have gained to offer an optimized solution for complex network infrastructures, such as fixed line/mobile service providers and large-scale enterprise networks.

NetQuest Corporation

523 Fellowship Road
Mount Laurel, NJ 08054 USA
+1 856.866.0505

info@netquestcorp.com