NetQuest and H+S Polatis Protect Customers from Cyber Crime with Automated Mass Optical Surveillance Solution

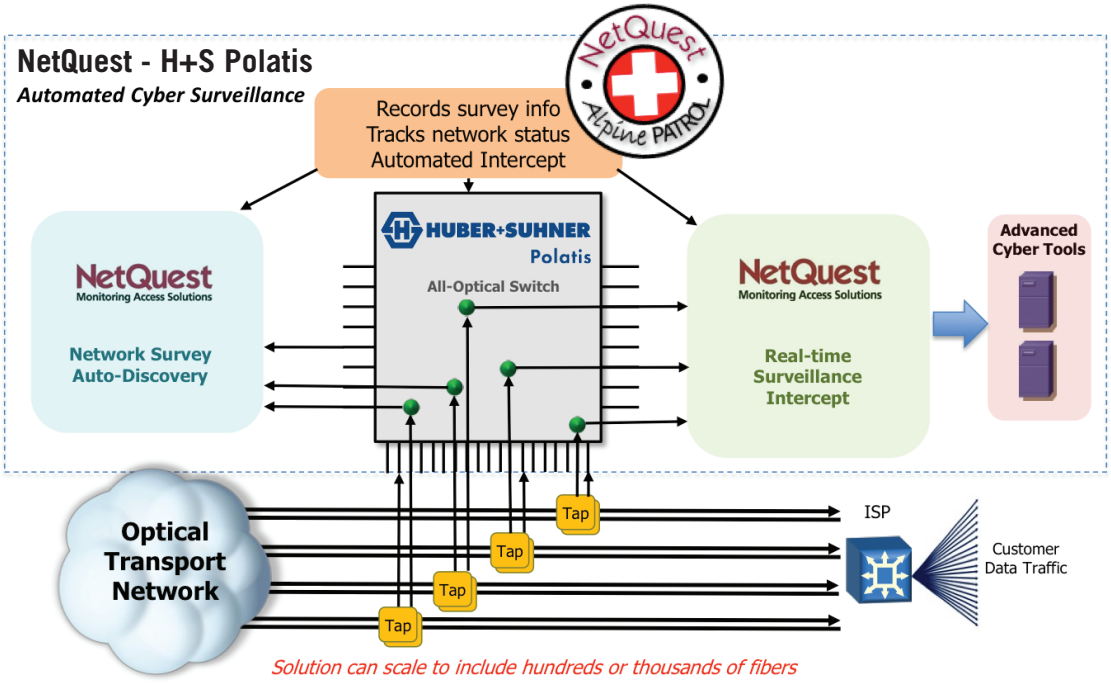
JOINT SOLUTION BRIEF

Overview

International government and business leaders have made it very clear that cyber-attacks are their new number one concern, even more so than terrorism. High profile attacks like WannaCry and Not Petya are forcing billions of dollars to be spent trying to avoid these types of crippling events. As governments and business increasingly rely on communications technology on all fronts, there is a growing dependence on the communications industry to deliver cyber solutions that can generate intelligence and increase security across a widening array of network architectures. And, with traffic volume skyrocketing with no end in sight over intercontinental submarine networks and emerging 5G mobile networks, the task of finding advanced threats is the cyber equivalent to searching for a needle in a haystack.

Solution

NetQuest and Huber+Suhner (H+S) Polatis have collaborated on an advanced automation technique for accessing big data carried over large scale optical transport networks. The joint solution combines NetQuest's unique blend of network survey and intelligent traffic intercept functions with H+S Polatis' high performance all optical switching technology to produce instant access to thousands of individual fibers for monitoring and analysis. By introducing automation to the optical network data access challenge via NetQuest's Alpine Patrol orchestration platform, NetQuest and H+S Polatis are providing broad visibility to an unprecedented volume of traffic and giving today's mission critical cyber tools a significant advantage in detecting advanced cyber threats.



The Power of Scale

H+S Polatis offers a wide array of all optical switches for direct connections ranging from 4 x 4 to 384 x 384 ports with ultra-low optical loss and superior performance. The switches are signal, bit-rate and format independent up to 100G/400G and beyond, which provides a future proof solution. Multiple switches can be cascaded to access even higher volumes of individual fiber links.

Previously, NetQuest Interceptors were limited in the number of fibers they could monitor by the number of physical ports on the appliance, typically with a maximum of 8-10 input connections. The joint surveillance solution can now be used to cycle through hundreds, or even thousands, of optical fibers and perform a full automated network survey effectively revealing the key signaling attributes of each of the optical communication signals. This network survey, or auto-discovery, of the optical network is a critical function that NetQuest is uniquely capable of revealing. The Interceptors can provide the following discovery information for each optical signal:

- Network/Fiber ID and signal presence
- Optical wavelength (i.e. ITU channel 16, etc.)
- Signal type (i.e. STM-64, 100GbE, OTU4, etc.)
- OTN and SONET/SDH channelization structure including transport OH
- Geo location and path ID (i.e. Russia to Brazil, etc.)
- Transport protocol and UDP port detection (i.e. GFP, POS, Ethernet, etc.)

Integrated Management

The combined automated solution utilizes NetQuest's Alpine Patrol orchestration platform to manage NetQuest Interceptor appliances and the high-density optical matrix switches from H+S Polatis. Individual optical fibers can be physically tapped and monitored by NetQuest through the H+S Polatis optical switch. Changes can be made in real-time instantly from one management console.

Alpine Patrol is constantly storing this survey information and tracking any changes to the network provisioning. This is especially critical while monitoring today's adaptive networks where signaling paths are constantly being re-provisioned to react to traffic bottlenecks and other network impairments. With a detailed network survey database intact covering the entire transport network, critical traffic intercept decisions can be made instantly based on real-time intelligence and these operations can be performed without a need for manual intervention. Based on the particular mission, traffic intercept options are available at varying network layers including an entire fiber, individual traffic segments or via detailed filtering rules targeting individual IP addresses or other traffic related parameters.

H+S Polatis
www.polatis.com
info@polatis.com
+1 844.765.2847

NetQuest
www.netquestcorp.com
info@netquestcorp.com
+1 856.866.0505

Why Deploy the NetQuest / H+S Polatis Solution?

The increasing damage being done by cyber related crimes is presenting global leaders with a crisis that demands to be combatted with innovative solutions. NetQuest and H+S Polatis's mass surveillance solution provides unique network visibility via a layer of automation that efficiently translates analysis of big data optical networks into actionable intelligence.

With H+S Polatis switches providing expanded visibility, NetQuest Alpine Patrol can provide comprehensive optical network analytics, both real-time and historical, using metadata extracted across the entire transport network. These analytics can be combined with analysis of individual IP flows to form a threat detection algorithm that accesses a much wider and deeper set of information for finding network anomalies and enables more intelligent network security decisions.