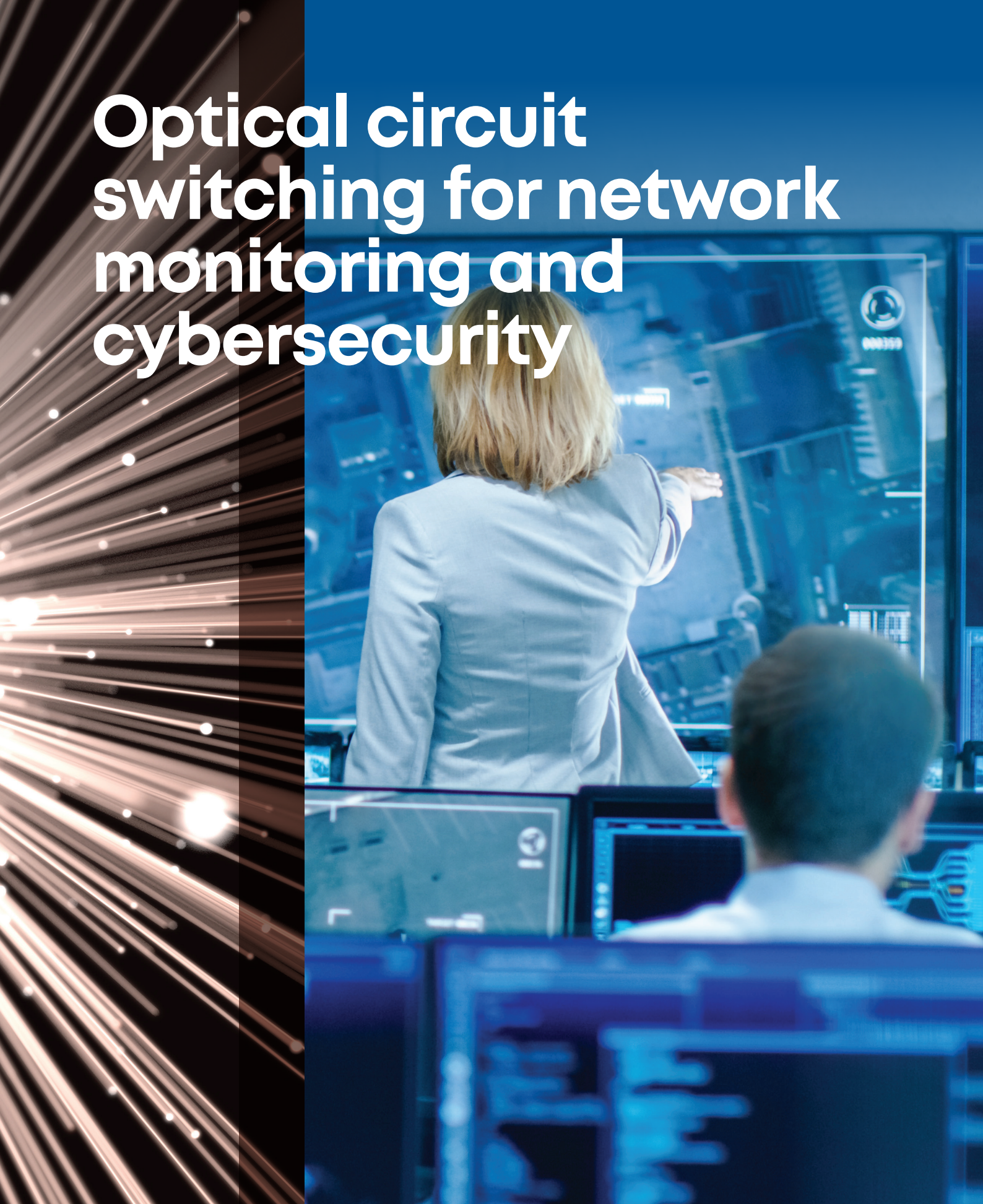# Optical circuit switching for network monitoring and cybersecurity

White Paper

HUBER+SUHNER

Ensuring network security with optical circuit switching

Growing data usage requires more visibility

Global internet usage continues to grow to record levels, having increased a thousand-fold since 2002. Over 5 billion people, 66% of the world's population, now have access to and use the internet around the globe. In the US alone 3,138,420 GB of internet traffic is generated every minute.

The explosion of internet traffic and users has made it increasingly difficult for commercial entities and governments to monitor internet traffic to identify and suppress cyber threats.

Commercial entities such as large data centers and telecom providers need to monitor traffic for cyber threats that can adversely affect their customers, such as banks, insurance companies, stock exchanges, health care providers, utilities, municipal authorities and the like.

Government entities responsible for law enforcement and foreign intelligence gathering have to sort through petabytes of internet and telecom traffic to find important pieces of information in order to support law enforcement and national security objectives.

Protecting privacy as well as adhering to laws and standards

In order to provide these network monitoring services, systems have been developed to locate and extract specific pieces of important information buried in mounds of other traffic while protecting the privacy of legitimate users.

In most western countries network monitoring operations are governed by strict privacy laws and typically follow ETSI or CALEA standards. These standards specify the controls necessary for the process of establishing the legitimacy of lawful tasking of collection systems and for the formatting of collected traffic information (phone numbers, IP addresses, etc) and monitored content.
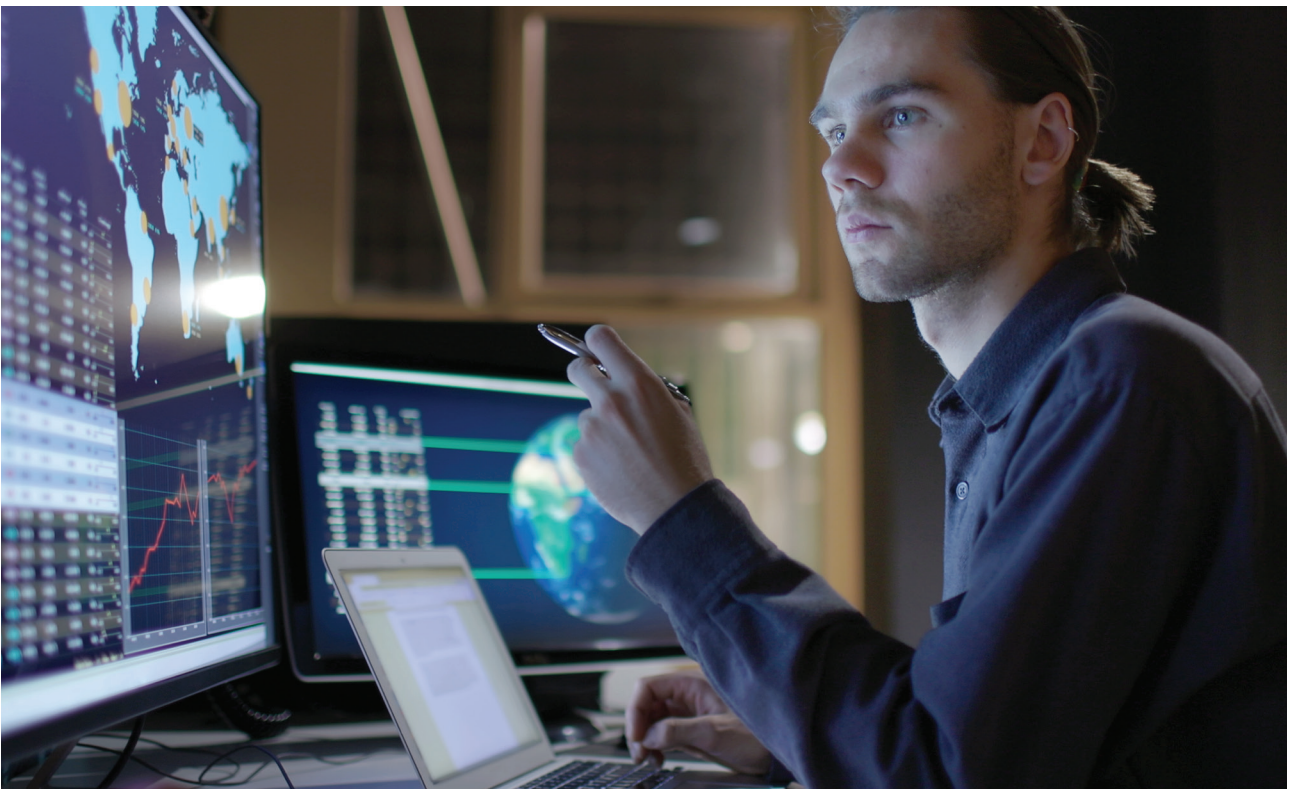
The challenge of cost effectively monitoring network traffic

The networks to be monitored, and the relevant point of intercept, can take on many different forms depending upon the type of network to be monitored.

The point of monitoring could be at a submarine cable landing station, in a carrier facility, internet exchange or data center, or on a network that is monitored for national security purposes. That location may be unmanned and possibly even remote.

In many of these applications the numbers of fibers to be monitored can be in the hundreds or even thousands. Each of those fibers can be carrying hundreds of gigabytes of traffic which challenges operators to sort through mountains of traffic in order to find specific information of interest, detect traffic that should not be on the network and identify and shut down cyber threats.
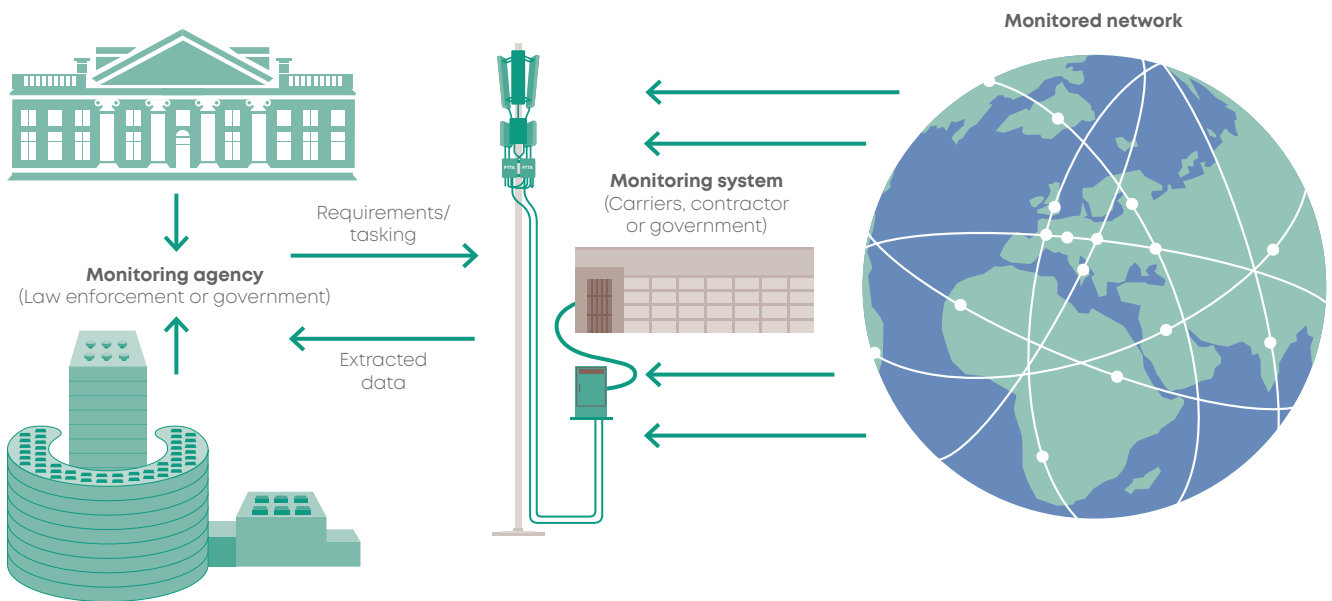
Simplified overview of network monitoring and intelligence gathering

The network monitoring process is complicated further by the wide variety of formats, data rates, wavelengths, protocols and encryption that are present across the links being monitored. Advanced analysis and collection tools operating at line rates are deployed to break down the traffic on any given link to be able to identify and extract the particular signals of interest, while making sure to protect the privacy of other users.

Ideally, these tools should be applied to every line traversing the point of monitoring in order to provide broad, real-time, network visibility. However, the huge number of lines to be monitored means that 100% monitoring can be cost prohibitive, particularly at line rates of 100 Gbs or more, as it requires a lot of equipment and human operators in the process.

Operators therefore require cost effective ways of sorting through large amounts of data. To accomplish that, they need to be able to leverage a smaller number of analysis and collection tools across the larger number of lines to be monitored, in order to utilize their expensive tools in the most cost-efficient way. A lower cost front end can be used to preselect which fibers are to be monitored and only forward those fibers involved in active survey or monitoring tasks to the tools and appliances that can extract the information of interest. In turn that information is forwarded to analysts or databases, securing a superior return on investment in these tools.

How optical circuit switching contributes to network monitoring

An efficient and cost-effective solution

An optical circuit switch provides a cost-effective solution for preselecting the fibers to be passed on to the network analysis appliances on an as-needed basis. The capability of the optical circuit switch to make signal-agnostic connections completely irrespective of the wavelength, protocol or data rate present on the fibers is essential.

An optical circuit switch can be used to route fibers to auto-discovery tools that can analyze the content of any given fiber and either forward the signal of interest for collection purposes or save the information to a database for further analysis. The fibers can be routed one by one to the auto-discovery tool on a rotating basis in order to build up a full picture of the types of traffic traversing the network over time. The database can then be monitored to provide insight as to where specific signals are located in the mass of network traffic. This allows the network monitoring administrator to perform a cost-effective network survey, and when a target is identified, the optical circuit switch can be commanded to direct that specific data stream to a persistent collection device for analysis and reporting.
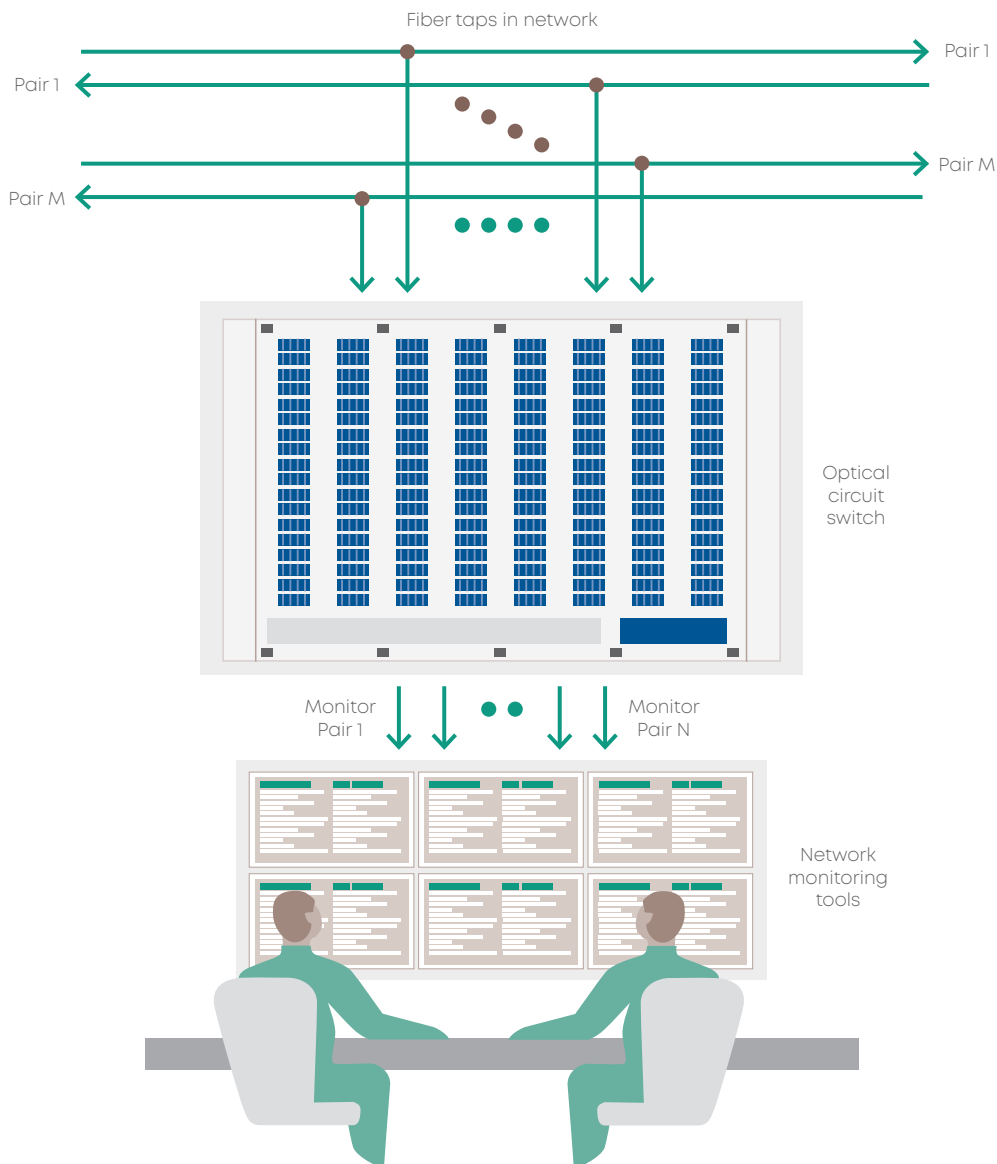
Optical circuit switch as intermediary between network taps and monitoring tools

The optical circuit switch of choice – POLATIS® from HUBER+SUHNER

The mission-critical component for network security

The highly dynamic nature of the network survey and collection environments requires optical circuit switches that switch quickly and provide superior long-term reliability. As the preselect element in these architectures, the optical circuit switch becomes a mission critical component of the network survey and collection system. POLATIS switches have been deployed thousands of times over the past 20 years and they continue to provide fast and reliable connections in support of many network monitoring applications.

In a typical application, the network fibers are passed through a passive optical tap which pulls out a small amount of the light on the fiber and directs it towards the collection system, thus allowing the bulk of the light to continue in the network and not degrade the network performance to any significant degree. The low level of the signals routed to the collection systems requires the connections through the optical switch to be as low loss as possible to preserve the integrity of the optical signals being analyzed. POLATIS optical circuit switches provide the lowest insertion loss available with typical losses of only 0.6 dB for switches with port counts up to 96x96. Larger switches still deliver best-in-class low loss performance.

Low loss is important, but it is also important that the fidelity of the collected signals is not impaired by the optical switch. This ensures the accurate collection and analysis of sensitive signals to support mission requirements. An optical circuit switch with stable connections that do not add noise to the signals traversing them is required and in this respect, POLATIS optical circuit switches are best in class.

Large port count optical switches are required to handle the large number of fibers typically present in network monitoring systems. The POLATIS range from HUBER+SUHNER provides the largest port count optical circuit switch available on the market today at 576x576. POLATIS switches are also available in asymmetric configurations such as 384x192 to support down-select configurations.

Leading vendors of network monitoring tools have fully integrated the software-defined POLATIS optical circuit switches into their system, creating an automated mass cybersurveillance solution.

Example of an Automated Cyber Surveillance System
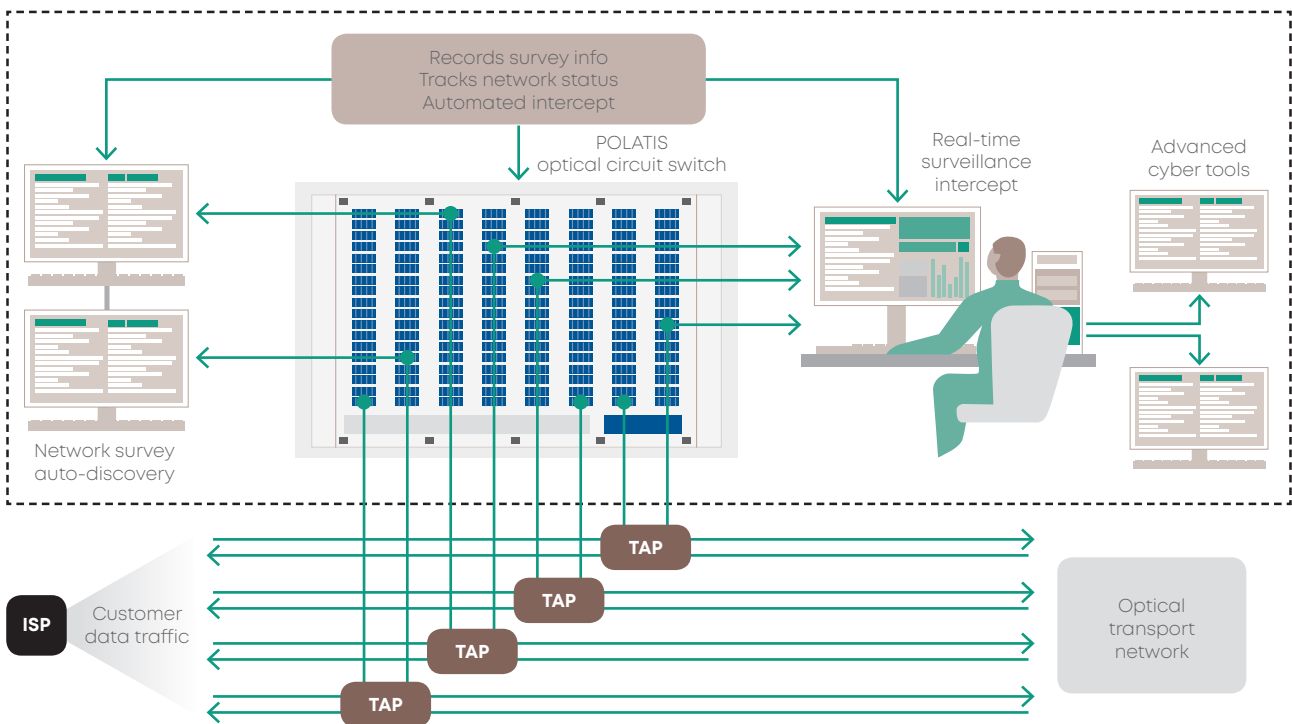
Solution can scale to include hundreds or thousands of fibers

POLATIS® optical circuit switching for network monitoring

Advanced and proprietary fiber optic switching technology

POLATIS® optical circuit switches have significant advantages over other all-optical (OOO) switching solutions for network monitoring, including:

- The industry's lowest optical loss and superior performance in stability, which are critical to ensuring signal integrity.
- The broadest range of symmetric (NxN) and asymmetric switches (MxN), in matrix sizes from 16x16 to 576x576 ports, essential to support the evolving needs of network monitoring, and with the potential to scale to survey tens of thousands of fiber connections.
- High density switch matrices occupying very little rack space.
- Protocol and data rate agnostic so can switch signals of any type.
- Switching time 25ms-75ms (subject to matrix size) for a single connection to support rapid cycling through multiple tap feeds.
- Near-zero signal latency for fastest delivery to network survey system.
- True dark fiber switching, which requires no light to make and hold connections, and is critical when switching low power signals, bidirectional or intermittent signals, and enables preprovisioning of future paths.

- Optional Optical Power Monitors, enabling measurement of the power of the signals passing through the switch.
- Optional Integrated Variable Optical Attenuation (VOA), which enables power levels through the switch to be managed to prevent damage to sensitive receivers.
- Support for the broadest range of Software Defined Networking (SDN) and command line interfaces, including TL1, SCPI, SNMP, NETCONF and RESTCONF.
- Fully software-defined for a seamless interface with leading cybersurveillance solutions.
- Robust by design to be highly reliable for mission critical applications, with dual redundant, hot-swappable network interface cards and power supplies.
- New POLATIS 576x576 switch also has dual redundant controllers and optional field addressable spare ports for increased resilience.
- Eco-friendly, low power consumption.
- Made in the UK and the EU.

POLATIS 576x576 Optical Circuit Switch with MTP Connectors

The HUBER+SUHNER advantage

HUBER+SUHNER Polatis has twenty years' experience globally in network monitoring and cybersecurity applications.

HUBER+SUHNER offers a broad range of products for network monitoring including network taps, fiber cables, patch cords, fiber management, structured cabling solutions, POLATIS optical circuit switches, WDM components and more.

Worldwide sales and support are available to make sure your network monitoring systems continue to operate day in and day out, providing the mission critical data needed to ensure effective law enforcement, intelligence collection and cyber security.