CASE STUDY

Mexican Mining Giant Gains Full Visibility into OT Infrastructure

KEYSIGHT

Organization

- Large company with mining, metallurgical and chemical operations across Mexico

Challenges

- Blind spots - not enough ports in security tools (OT sensors) to ingest all mirrored/tapped traffic
- Legacy switches unable to mirror traffic

Solutions

A comprehensive visibility solution, consisting of:

- Optical TAPs (Flex TAPs)
- Vision T1000 industrial packet brokers with support for sub-1G speeds
- Vision E40 packet brokers with support for 1G/10G/40G speeds

Results

- Optimization of existing OT security investments
- Full network visibility into all OT infrastructure components

The modernization of operational technology (OT) systems in addition to the increased automation of industrial control systems (ICS) have created an explosion of network-connected equipment. This can expose industries and their critical infrastructure to a wide range of cyber threats from nation states, criminals, disgruntled employees, and accidental misconfigurations. Further, OT networks and ICS were physically separated from traditional IT infrastructure are increasingly interconnected, creating unique security issues.

Ransomware, extortion, and financially motivated cybercrimes top the list of threat vectors that concern industrial cybersecurity teams. A successful ransomware attack, for instance, can be damaging to an organization on multiple fronts: the attack can interfere with and disrupt command and control of critical data and infrastructure, and attackers typically demand millions of dollars from the victim in exchange for restoring access to data and/or operations.

There has never been a more pressing need for industrial cybersecurity teams to monitor and protect their organization’s critical infrastructure and systems.

Situation and Key Objectives

With over twenty mining, metallurgical, and chemical plants across Mexico, this large industrial operator has a significant OT infrastructure that needs to be monitored and protected. In response to expanding threat vectors and rising threats, the customer launched a company-wide cybersecurity program that looks to strengthen internal cybersecurity capabilities, with the goal of reducing cybersecurity risks. The program initiatives can be mapped to the NIST Cyber Security Framework and grouped under four elements: *Prevention* (opportunities for cybersecurity improvement and strengthening), *Detection* (continuous monitoring and cybersecurity vulnerability management), *Identification* (e.g., asset inventory, etc.) and *Remediation* (e.g., corrective actions planning).

As part of *Prevention*, *Detection* and *Identification* initiatives, the company's OT security team procured a sensor-based OT security solution that combines behavior-based anomaly detection with signature-based threat detection. The company initially tried to leverage SPAN ports to supply OT security sensors with packet streams, but quickly ran into several limitations:

- OT security sensors not having enough ports to ingest all the mirrored traffic. While the customer had the option to deploy additional OT security sensors, i.e., more ports, inserting a visibility platform was a more flexible, simpler, and cost-effective option.
- Some legacy switches were incapable of mirroring traffic.

Keysight was selected to provide enhanced network visibility and to ensure the OT security sensors received all the relevant traffic - no blind spots. The Keysight visibility team collaborated extensively with the firm's OT security team, and the OT security solution vendor, on a visibility design that addressed existing blind spots, while also ensuring flexibility for future visibility needs.

The Visibility Solution

Flex TAPs were deployed to access traffic from optical links across various locations. Keysight Flex Tap passive fiber optical TAPs provided an exact copy of network traffic, without impacting equipment on the network, ensuring a seamless, reliable capture of traffic.

Keysight Vision NPBs (network packet brokers) were deployed at each of the company's plant locations. Positioned between the traffic acquisition points and the OT security sensors, the Vision packet brokers function as a packet distribution layer, aggregating, replicating, and redirecting the acquired traffic to the different OT sensors.

More specifically, Keysight Vision E40s and Vision T1000s packet brokers were deployed:

- With 20 x 100M/1000M and 6 x 10M/100M/1000M ports, the Vision T1000 industrial packet broker allows for the aggregation and monitoring of sub-1G links which are still widely used for OT/ICS applications. Further, the VT1000 is designed to be deployed in harsh environments, allowing the customer to deploy these packet brokers in locations that have a wide range of environmental requirements.
- With support for 1G/10G/40G port speeds and up to 48 ports, the Vision E40 is used to aggregate traffic from 1G links. Further, the Vision E40s are set to accommodate future aggregation needs as the company upgrades speeds in the OT environment.

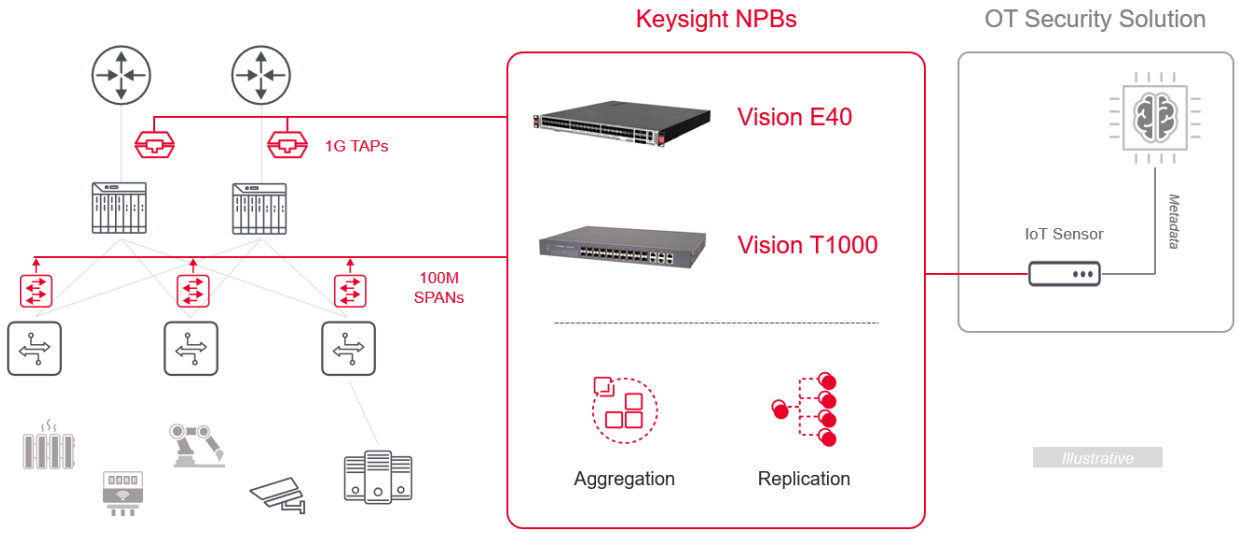

Figure 1. Initial large OT site configuration (illustrative)

Results

By deploying Keysight's visibility solution, the customer was able to address blind spots and cost management challenges associated with not having enough ports on the existing OT security sensors. The Vision NPB aggregation and replication capabilities significantly reduced the number of sensor ports needed to ingest all mirrored traffic, allowing the customer to save the cost of purchasing more sensors and to get the most out of the existing OT security solution.

Keysight optical TAPs also helped the customer overcome SPAN limitations in legacy switches, allowing for 100% of network traffic to be monitored and analyzed by the OT security sensors.

With the breadth and depth of Keysight's visibility portfolio and ecosystem of partners, industrial asset operators and owners can monitor their OT infrastructure for cybersecurity threats. From network TAPs to network packet brokers, Keysight can mix and match products to deliver the right visibility solution for IT and/or OT environments.