SUCCESS STORY

Mexican Mining Giant Gains Full Visibility and Strengthens Security of OT Infrastructure

Organization

- Large company with mining metallurgical and chemical operations across Mexico

Goals & Challenges

- Gain complete OT visibility for improve cyber resilience and reduced cyber risk
- Deploy an efficient monitoring solution architecture — existing environment characterized by high switch count

Solutions

- Nozomi Guardian sensors and Nozomi Central Management Console (CMC) deployed on-premise
- Keysight visibility solution consisting of optical TAPs, Vision T1000 industrial packet brokers and Vision E40 aggregation packet brokers

Results

- Full visibility into all OT infrastructure components
- Enhanced operational insights and threat detection capabilities
- Optimization of existing OT security investments

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

The modernization of operational technology (OT) systems and the increased automation of industrial control systems (ICS) have created an explosion of network-connected equipment. Further, OT networks that were physically separated from traditional IT infrastructure are increasingly interconnected, creating unique security issues and risks. These transformations expose industries and their critical infrastructure to a wide range of cyber threats and attacks, with ransomware, extortion, and financially motivated cybercrimes topping the list of concerns for many organizations.

Situation and Key Objectives

With mining, metallurgical and chemical locations across Mexico, this large industrial operator has a significant OT infrastructure that needed to be monitored and protected. In response to expanding and rising threats, the organization launched a corporate program that looked to strengthen internal cybersecurity capabilities and enhance vulnerability management and response, with the ultimate goal of reducing risk.

One of the program's major initial initiatives was to implement continuous and permanent monitoring of all infrastructure assets for improved detection and response to cybersecurity threats. Following extensive testing and validation, the company's security team procured Nozomi Network's OT visibility and monitoring solution. Nozomi Guardian and Nozomi Central Management Console provide accurate asset inventories, associated vulnerabilities, and real-time anomaly and threat detection across the OT environments.

The Keysight and Nozomi Networks Joint Solution

As a first step, Nozomi Guardian sensors were deployed at all sites in all locations to monitor the OT infrastructure. The Nozomi Guardian sensors analyze network traffic passively and provide a real-time view into the OT environment. Next, the Nozomi Central Management Console (CMC) was installed on premise at a one site to aggregate asset and alert data into a single place, and for security teams to manage and update all sensors.

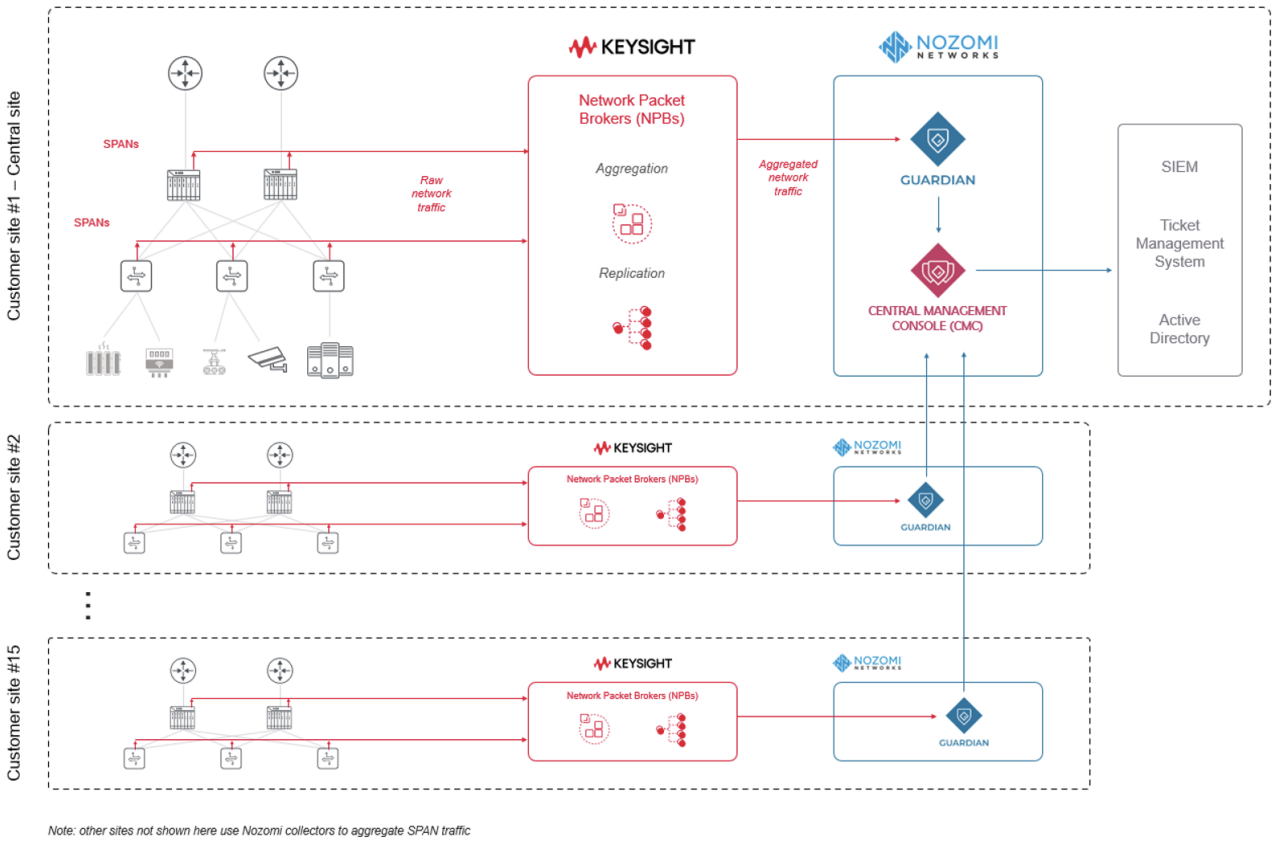

Figure 1. Site configuration (illustrative)

The initial plan was to leverage SPAN ports from multiple switches at each site to supply local Guardian sensors with the required traffic. However, the number of SPAN ports needed for complete traffic visibility at some sites exceeded initial calculations, which in turn would require the addition of more Guardian sensors at these sites.

After evaluating options, the company found that inserting a visibility platform was the most flexible, simple and cost-effective option to capture mirroring traffic from a large number of switches. Keysight was procured to provide enhanced network visibility and to ensure the Guardian sensors at the relevant sites received all the relevant traffic – i.e., no blind spots. Keysight network packet brokers (NPBs) were deployed between the traffic acquisition points and the Nozomi Guardian sensors. These NPBs function as a packet distribution layer, efficiently aggregating, replicating, and redirecting the acquired traffic to the Nozomi Guardian sensors.

Results

Tangible benefits of deploying Keysight's visibility solution alongside Nozomi Network's solution include:

- Full visibility and monitoring of OT assets across all sites, despite network switch limitations and quantities
- Enhanced operational insights and threat detection capabilities necessary to ensure the resilience and continuity of the company's industrial operations
- Automated real-time notification of anomalies and advanced threats
- Optimization of existing OT security investments by simplifying the monitoring solution architecture

Visit **GetNetworkVisibility.com** for the latest from Keysight on insights for optimizing network monitoring, security, and analysis.

For more info, contact: 1-888-438-4942 or visibilitysales@keysight.com