CASE STUDY



Middle Eastern Power and Water Authority Upgrades Visibility

Optimized Traffic Delivery Modernizes OT Security Monitoring

KEYSIGHT

01

Industry

Government-owned utility

02

Company

Provider of water and electricity to residential and business customers across a major Middle Eastern city

03

Problem

Scaling and modernizing security monitoring in OT environments

04

Solution

Deploy Nozomi Guardians at major power substations with Keysight optimizing traffic for threat detection and response

Overview

For government-run utilities operating their nation's critical infrastructure (CI), outages due to cyberattacks are simply not an option. One Middle Eastern power and water authority partnered with Nozomi Networks and Keysight to help improve its detection and response to events that could take down the city's public safety networks, fire alarms, and citywide transportation systems.

With cyberthreats targeting the region's CI on the rise, the authority decided to modernize its monitoring of operational technology (OT) security to reduce risk and improve resilience. Step one was deciding to deploy an OT security monitoring solution at 14 substations across a major city to help accelerate threat detection and incident response.

After evaluating solutions from several leading providers, the authority chose to move forward with Nozomi Networks, a global leader in critical infrastructure and OT security monitoring. That decision led to step two: optimizing network traffic for analysis by Nozomi Guardian sensors.

The Challenge

Scalable, Cost-Effective Capture, Filtering, and Delivery of Data to Nozomi Guardians

The power and water authority's security operations team knew the Nozomi Guardians needed full visibility into traffic flowing across and between IT and OT systems to effectively detect malware and advanced threats. Deploying hardware-based monitoring at each substation would prove cost-prohibitive, so the team sought a viable alternative.

The ideal design called for capturing, aggregating, and filtering traffic at the edge, then performing centralized visibility functions to remove unwanted traffic and lower cost. Key visibility requirements included:

- Complete coverage across distributed substations
- Efficient traffic capture and aggregation
- Centralized optimization and cost-efficient delivery of traffic for analysis
- Elimination of unnecessary data prior to analysis

The team elected not to conduct a proof-of-concept demonstration. Instead, they chose to deploy a Keysight network visibility platform based on real-world evidence:

- Keysight's reputation for success partnering with the nation's government-run agencies
- A long track record of successful collaborations between Nozomi Networks and Keysight helping to secure OT environments
- The ability of Keysight solutions to minimize hardware requirements while scaling aggregation to 48 ports

The Solution

Filtering Traffic for Fast, Reliable Analysis

After a detailed site survey to optimize the deployment, the implementation proceeded quickly within a few weeks.

How the Architecture Works

The new three-part network visibility solution that optimizes traffic for analysis includes:

- Traffic collection at the edge using Keysight network taps deployed across 14 substations
- Edge aggregation and filtering performed by Keysight Vision Edge 40 network packet brokers to filter out non-security-relevant data (e.g., CCTV streams and OT protocols) not required for threat detection and optimize bandwidth utilization in sending traffic upstream

- Centralized, advanced network visibility using a Keysight Vision ONE packet broker to:
  - Remove duplicate packets
  - Send clean traffic to Nozomi Guardians for analysis
  - Improve bandwidth and tool utilization even further
  - Support Nozomi Guardian sensors that observe and analyze network traffic to deliver asset visibility, threat detection, and centralized monitoring

City's Critical Infrastructure Better Protected

By improving access to relevant threat data while avoiding the deployment of hardware monitoring stacks at every site, the joint Nozomi Networks–Keysight solution delivers:

- Scalable coverage without driving up cost
- Strong return on investment (ROI)
- Improved centralized management and operational stability

Next Up

More Sites, Stronger Security

With its scalable visibility and OT security monitoring architecture in place, the authority is well positioned to:

- Extend coverage to additional substations
- Integrate future OT security tools
- Defend against increasingly advanced, AI-led cyberattacks

Visit https://www.keysight.com/us/en/products/network-visibility.html for the latest from Keysight on insights for optimizing network monitoring, security, and analysis.

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

As a mission-critical design enablement partner, Keysight connects design, emulation, and test so customers can solve the world's most complex engineering challenges. Accelerate innovation at www.keysight.com.

KEYSIGHT

This information is subject to change without notice. © Keysight Technologies, 2026, Published in USA, October 26, 2026, 3126-1900.EN