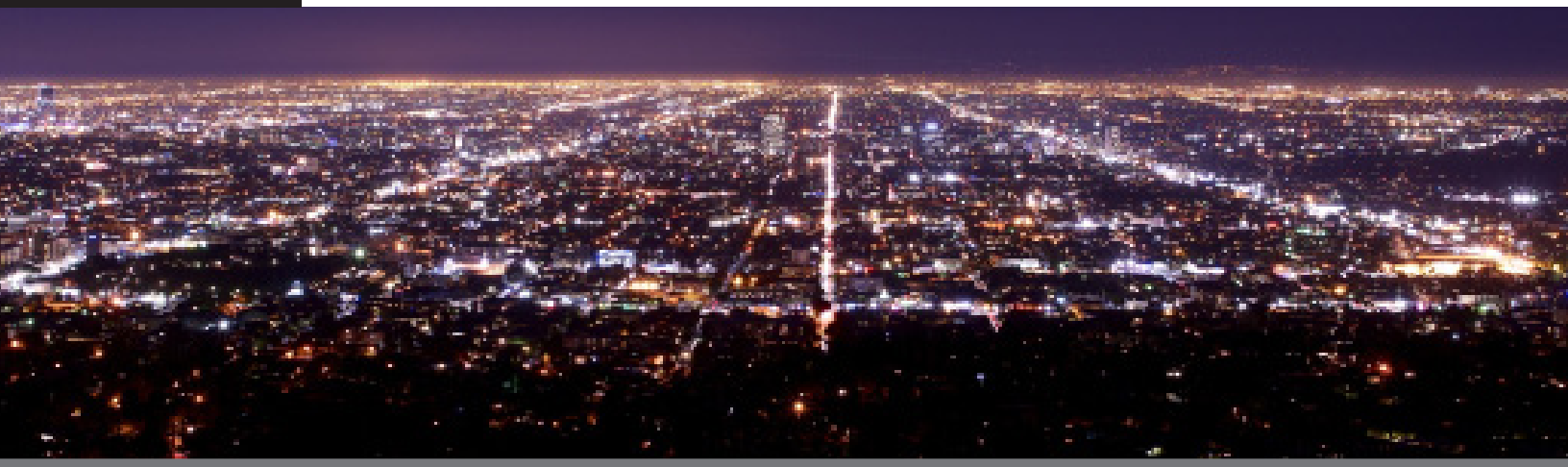

SUCCESS STORY

North American Utility Company Upgrades Power Plant Security with Keysight Visibility Fabric

COMPETITIVE TAKEOUT

HIGHLIGHTS

Industry: Industrial

Customer: North American Utility Conmpany

Highlights:

- Highly sensitive data used to regulate the flow of energy across the power grid delivered reliably and efficiently
- Monitoring traffic capacity requirements reduced nearly 90%
- Easy transition of support to Security Operations Center (SOC) team
- Provider positioned for compliance years ahead of CIP-015 regulations for monitoring critical infrastructure

A regional electricity provider upgraded its network visibility and monitoring to ensure real-time visibility, improve threat monitoring and detection, and gain a massive head-start on impending cybersecurity regulations.

A North American electricity company chose to upgrade its monitoring capabilities across its serving region to ensure visibility of control systems that regulate the flow of power through the grid and control power generation equipment. To maintain power quality and avoid potential shutdowns, sensors measure values such as speed of turbines and electric frequency 60 times per second or faster. The resulting data can overwhelm a monitoring system.

The new monitoring infrastructure features a Keysight visibility fabric spanning 15 power plants, energy management systems (EMSs), and substations connected to industrial cybersecurity monitoring solutions from Dragos. The provider began installing its Dragos technology several years ago to monitor for signs of foreign attacks on the power grid.

The strategic investment also laid the groundwork for compliance with impending CIP-015 regulations. The new Critical Infrastructure Protection (CIP) rules aim to improve security across the power grid by requiring Internal Network Security Monitoring (INSM) be in place for all high- and medium-impact systems.

That's where world-class visibility comes in...

Cybersecurity architects led the charge

Company management and Risk Management Personnel had been tracking the increasing number of threats and requested a solution that provide enterprise-wide monitoring of operational technology (OT) systems. In response, the Security architects at the electric company proposed expanding monitoring capabilities to achieve greater visibility across OT environments in order to detect and interdict the types of attacks that caused massive shutoffs in other countries. The team presented an INSM solution to the provider's Board of Directors and Risk Committee as part of a larger visibility solution encompassing both network and endpoint monitoring. The INSM system collects and filters traffic from the network and funnels it to Dragos monitoring solutions used to flag malicious traffic.

Prior to upgrading to Keysight's Vision network packet brokers (NPBs), the company had installed Cisco technology that was able to collect and send a all network data to the Dragos systems — but the stream proved highly inefficient. The solution lacked the ability to remove duplicate data packets, which are very common in control system environments, and offered limited capabilities for filtering out unnecessary backup traffic and other unwanted information that consumed valuable network and monitoring resources.

"Now, after implementing the Keysight deduplication the monitoring tools just see one packet which takes a tremendous processing burden off of the Dragos equipment. We're also achieving a high signal-to-noise ratio...." *— Security Architect*

The utility company had already chosen Keysight as its 'corporate standard' for visibility across its IT environment and the team saw no reason to change directions in extending capabilities across OT networks. Along with superior advanced traffic filtering capabilities, the Keysight solution and user interface (UI) deliver industry-best ease of use.

"We initially thought the implementation team would turn over support for this system within a year or two following deployment," one cybersecurity architect recalls. "Supporting the previous solution was so complicated we knew we couldn't turn over maintenance to our security operations center (SOC) because it would take up too much of the team's time. We were aware that support might be a liability going in but were hoping to make the job easier with Keysight as well."

Massive efficiency gains achieved

With Keysight in place providing granular advanced filtering, the team witnessed a massive reduction in the volume of traffic bombarding its monitoring architecture and security tools. "Before replacing the old solution with Keysight, we had one location with 14 switches receiving the same data 14 times," the security architect explains. "Now, after implementing the Keysight deduplication the monitoring tools just see one packet which takes a tremendous processing burden off of the Dragos equipment. We're also achieving a high signal-to-noise ratio," the architect continues. "The signals are all things we want to monitor and the unwanted noise effectively gets filtered out."

After deploying Keysight in one location, monitoring traffic capacity volumes dropped from above 1Gbps to an average of 175Mbps almost immediately. Deduplication improved and the team was able to adjust and apply advanced filters to remove backup packets, replication traffic, and other unwanted information. After these improvements, the Security Operations Team is able to find relevant data faster during exercises. In addition, tools that store network packet capture data are now able to retain data for much longer – as much as an additional week – after filtering low value data from the network data feed.

And, it was easy . . .

The security architect reports his team was able to pull out the old solution and plug in Keysight Vision packet brokers within minutes. “Keysight’s interface and the usability of the system are phenomenal compared to what we had,” recalls the project lead. “With the previous solution we spent a bunch of late nights getting things to work. With Keysight we held one training meeting that took less than an hour and everyone was able to get things up and running with no trouble. The interface does what it’s designed for: we just plugged it in and everything worked.”

Operating the Keysight platform proved so simple the architecture team was ready to turn over support to the SOC team sooner than expected. “We want that team to be spending its time looking at the data to find potential threats, not supporting the systems that send them the data,” the architect explains. “We set aside an hour to show them the new Keysight interface and after ten minutes they were 100 percent onboard with accepting responsibility for support.”

Last but not least, the power company appreciated the continuity of being able to work with the same Keysight team throughout the planning and implementation of the new visibility solution. The combination of advanced feature functionality, ease of use, and dedicated support reinforced the company’s choice of Keysight as its long-term visibility partner in both IT and OT environments into the future.

“The convergence we’re seeing is not one of IT and OT networks but of the technologies used within each environment,” the security architect concludes. “For example, the use of a laptop running Windows inside a power plant. As that convergence continues and new mandates for monitoring data take effect, we believe we’re years ahead of the game with our solution from Dragos and Keysight.”

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