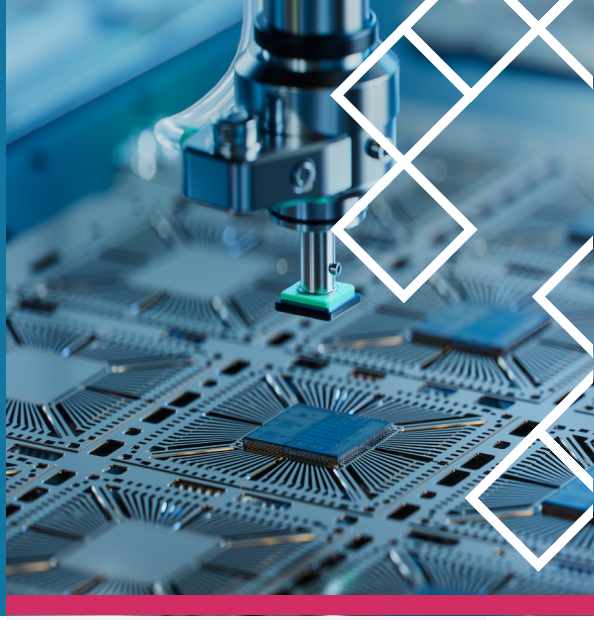
NOZOMI NETWORKS

KEYSIGHT TECHNOLOGIES



CASE STUDY

Keysight Turns to Nozomi Networks to Strengthen Its Production Line Defenses

Customer Profile

- A global test and measurement equipment manufacturer (headquartered in the U.S.)
- 10+ manufacturing sites in North America, Asia, and Europe
- 20K+ employees

Goals & Challenges

- Integrate and streamline effective IT and OT security management to improve ROI
- Strengthen operational and supply chain reliability and cybersecurity resilience
- Automate insurance compliance reporting related to asset inventories

Results

- Cut OT incident response times by 50% with AI-powered targeted alerts
- Improved Keysight's ability to identify and accurately classify assets by 50%-70%
- Eliminated hundreds of hours of manual labor each month/year by automating precise, real-time asset inventory tracking
- Keysight's IT Security team has full visibility into OT networks and has simplified the holistic management of IT & OT security with a deployment architecture that aligns with current and future security requirements

Keysight Technologies is driving operational resilience for the long term with an OT & IoT security solution that offers both deep and broad visibility across all of its manufacturing facilities and systems.

Keysight streamlines advanced IT & OT security management and response for electronics manufacturing and assembly.

Vantage and Vantage IQ Give Keysight Global OT Visibility and AI-powered Cybersecurity Analysis

The Challenge: Enterprise-wide Device Fingerprinting & Accurate Asset Inventories

Keysight Technologies' manufacturing facilities use device fingerprinting and asset inventories for cybersecurity and insurance purposes. Before deploying Nozomi Networks, the information had to be generated and updated manually. Because this process required hours of extensive manual auditing, updates could be made only periodically. It was also difficult to detect new devices over time, generate a vulnerability registry, and translate data into actionable activities.

The cybersecurity team at Keysight Technologies wanted to solve this problem with a solution that could:

- Provide in-depth visibility and analysis needed to accurately identify all the assets running in Keysight's manufacturing plants worldwide.
- Automate the process of maintaining a real-time asset inventory across all of its facilities.
- Easily deliver an accurate and up-to-date asset registry at any time.
- Provide actionable insights to support a faster, more targeted response to anomalies and threats.

The Solution: Cloud-based Asset & Network Visualization with Asset Intelligence Enrichment

Nozomi Networks worked closely with Keysight Technologies to address the manufacturing system's visibility challenges. Vantage was deployed to provide a consolidated view of all assets, networks, and vulnerabilities across Keysight's worldwide manufacturing facilities.

Asset inventory accuracy and depth was a priority. To complement device fingerprinting and asset enrichment performed at the edge, Vantage's asset intelligence enrichment engine was enabled, which leverages cloud-powered artificial intelligence (AI) to identify unconfirmed assets based on confirmed asset data and correlated asset behaviors. When an unconfirmed asset's behavior aligns with certain criteria, asset details such as type, vendor, and product name can be determined with a high level of confidence.

Keysight Technologies reported an impressive 50%-70% average improvement in its ability to identify and accurately classify assets after activating Nozomi Networks' asset intelligence enrichment. The real-time asset inventory and vulnerability data informs Keysight Technologies' broader security decisions and significantly reduced the manual labor previously required.

Keysight Technology Taps and Packet Brokers with Nozomi Guardian Sensors

The Challenge: Comprehensive IT and OT Network Traffic Collection On-Premises

Keysight Technologies wanted to leverage existing security tools in its Security Operations Center (SOC), IT and OT networks. It was imperative that an OT security solution fit cohesively into the existing architecture.

In addition, the Nozomi Guardian sensors use network traffic as a data source for anomaly and threat detection which cannot always be collected from a network switch due to switch capabilities.

Keysight Technologies needed an OT network monitoring and response solution that could:

- Address unique OT monitoring and asset identification requirements without slowing down manufacturing processes.
- Extend the use of OT network data to support anomaly and threat detection.
- Integrate easily with existing SOC, IT and OT security for efficient cybersecurity management company-wide.

The Solution: Taps and Packet Brokers for Traffic Collection to Guardian Sensors

Keysight deployed its own products, taps and network packet brokers, in its IT environment to monitor network traffic. This ensures:

- Data collection does not impact existing network infrastructure performance.
- No switch interfaces are consumed by port mirroring (SPAN) configuration.
- Traffic could be aggregated, de-duplicated and filtered prior to transmission to maximize the performance of the Nozomi Guardian solution.
- Network traffic can be used for other purposes at a later date.

A single Guardian sensor is used to monitor the entire facility for asset and vulnerability visibility, anomaly detection and signature threat detection. This simplifies management and maintenance for the platform and ultimately reduces TCO of the solution for Keysight's entire IT and OT cybersecurity practice.

AI-Powered Alerts and Analysis for Fast, Targeted Incident Response

The Challenge: Strengthen Operational and Supply Chain Reliability and Cybersecurity Resilience

With OT cyberthreats on the rise, relying on traditional enterprise security controls for the OT environment was no longer sufficient and posed a significant risk to Keysight Technologies' overall business. To address the challenge, an executive-led initiative was launched to identify ways the existing Security Operations Center could be leveraged to protect the business's operations and supply chain from cybersecurity risk.

Keysight aimed to:

- Leverage the existing SOC to receive and review security events detected in the OT environment.
- Expand the scope of SOC monitoring to include OT in a cost-effective way.
- Reduce the mean time to resolution for potential OT cybersecurity incidents through rapid detection.

The Solution: The Nozomi Networks Platform Empowers Keysight Technologies

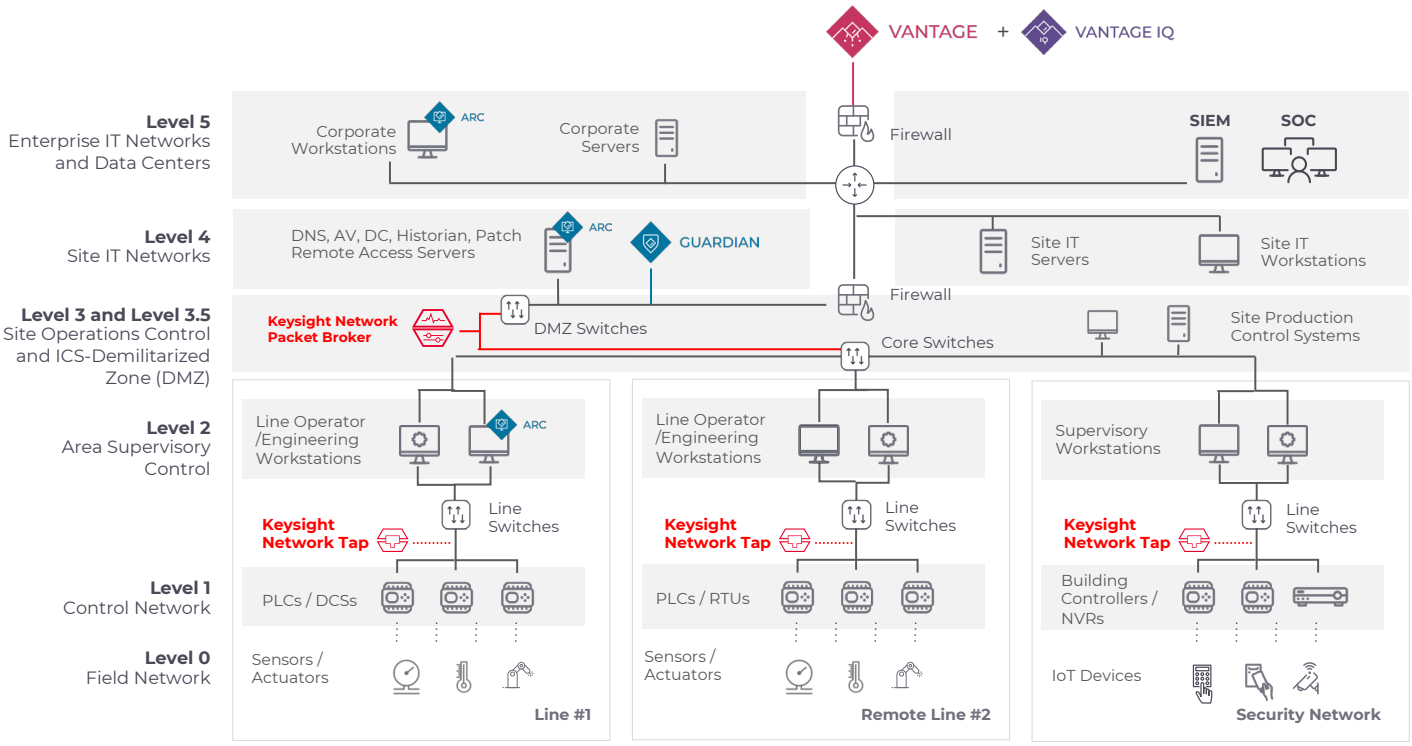
The Nozomi Networks platform detects both anomaly-based and signature-based alerts and transmits those events to the Keysight Technologies Security Operations Center in real-time. Machine Learning models in the Guardian network sensor correlate detections that are related with a high confidence threshold. Furthermore, the Vantage IQ AI engine performs ongoing analysis of the current and historical dataset of alerts, providing insights such as changes in alert patterns over time, dramatic increases in the quantity of high-risk alerts at a facility, and identifying when multiple events indicate a confirmed incident with high likelihood.

Keysight Technologies Security Analysts are empowered with event data as it occurs in the OT environment. Data may be incorporated into the SOC's review and escalation processes to enable the business to dramatically reduce the effort and time required to identify security threats. AI-powered insights in the platform enable the existing team to evaluate a larger volume of data and dramatically reduce the time-to-value of Keysight's investment.

"The Nozomi Networks platform was the right solution for both deep and broad visibility of our manufacturing systems. The solution, which also leverages Keysight taps and packet brokers, maximizes the value of our investment, fits all facilities and systems, and has a meaningful impact on our long-term security position."

Ed Parkin
Senior Cybersecurity Architect, Keysight Technologies

Sample Architecture



KEYSIGHT

About Keysight Technologies

Keysight is your innovation partner, delivering market-leading design, emulation, and test environments that help you develop and deploy faster, with less risk, throughout the product life cycle. Push the boundaries of engineering and deliver the best product experiences with our fusion of technologies, measurement expertise, and tailored solutions built from a foundation of co-innovation with industry ecosystem leaders. Gather insights sooner to build and go to market with confidence.

Learn more at **keysight.com**

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI powered analysis for faster, more effective incident response. Customers rely on us tominimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com