Nozomi + Keysight: Visibility to Secure ICS and IoT

With the Internet of Things (IoT) bringing industrial operations online for the first time, network visibility and security must monitor and secure new devices. Nozomi Networks brings real-time visibility across industrial control systems (ICS), with Keysight ensuring reliable access to vital data from networks and devices.

Without complete visibility, detecting complex threats that develop over time across large volumes of historical data proves nearly impossible. A lack of integrated investigation and mitigation workflows also adds cost and complexity to operational technology (OT) security. The joint Nozomi Networks and Keysight solution offers OT visibility for both physical and virtual networks, with the choice of on-premise or SaaS management.

Joint solutions integrating Nozomi Networks and Keysight technology improve security at power substations, oil and gas facilities, discrete manufacturing sites, and other remote industrial locations. Together, we deliver the rich contextual insight needed to defend control networks against cyberattacks, undetected failures, and costly outages.

Highlights

- Achieve real-time operational visibility.
- Accelerate incident response.
- Improve ICS cyber resiliency.
- Save time and reduce effort.
- Achieve improved operational uptime.
- Avoid physical and virtual visibility gaps.
- Discover vulnerable IoT devices.
- Deploy flexible SaaS or on-premise operation.
- Choose among industrial grade deployment options.
Nozomi: AI-Powered ICS Security

Nozomi Networks delivers ICS cybersecurity solutions worldwide, providing comprehensive asset visibility, network monitoring, and cybersecurity detection for industrial networks. Nozomi’s Guardian solution features a suite of application modules to visualize, monitor, detect, and remediate cyberthreats in real time.

Guardian is the first ICS visibility solution powered by artificial intelligence (AI). It offers nonintrusive visibility across ICS and SCADA (supervisory control and data acquisition) environments, including multiple geographically separated plants, without adding latency, determinism, or jitter to the control network. Now with Vantage, Guardian can either be connected to the on-premise Nozomi Networks console, or with a cloud-based dashboard. With new alternative network options available, network owners and operators can configure a solution to address the needs of digital transformation and convergence projects. The combined and flexible solution delivers consolidated OT visibility, automatically learning all assets and working with your cybersecurity infrastructure to monitor networks and detect threats and anomalies.

Figure 1. Detect, prioritize and resolve threats to ICS and IoT infrastructures. With Nozomi Networks and Keysight, data collection occurs across multiple levels in your ICS environment. Nozomi Networks Guardian uses Keysight’s visibility architecture to capture comprehensive data and eliminate network blind spots. Nozomi Networks management, offered in on-premise or SaaS options, consolidates data to provide a comprehensive threat detection and analytics dashboard.
Keysight: The Right Data for the Right Response

Keysight network visibility solutions deliver complete access to both OT and IoT networks. Complete, real-time visibility starts with “tapping” networks to capture and copy traffic used in performance and security monitoring, incident response, forensics, and analysis.

To ensure complete visibility, tapping can occur in places where OT switches cannot adequately mirror packets. Keysight Taps may also substitute for data diodes because they allow copies of traffic to flow out of the monitored network segment but not back into it. In addition Keysight Virtual Taps allow for monitoring of virtualized portions of the network, such as HMI or other resources running on VMWare.

Data from the Taps, Virtual Taps, and switch mirrors flow to Keysight’s network packet brokers (NPBs) for real-time processing and delivery to Nozomi Network Guardian. Preprocessing of traffic includes removing duplicate packets and stripping unwanted or privileged data to improve overhead and meet compliance mandates for securing information. Keysight Taps and NPBs are available in Industrial grade options, suitable for the harshest environmental and certification requirements.

NPBs aggregate, process, and deliver to Guardian all relevant data from mirror and Tap and Virtual Tap connections, filtering out traffic not relevant to SCADA security (such as closed-circuit TV video over IP traffic). Packet Brokers can integrate with security information and event management with other systems to establish automated threat responses to indicators of compromise. Keysight network visibility also works with tools such as firewalls to improve policy enforcement and mitigate unwanted traffic.

Joint Solution Highlights

Together, Nozomi Networks and Keysight deliver comprehensive, highly automated visibility that helps defenders respond quickly, with confidence, every time. The joint solution allows you to do the following:

- Detect attackers in real time to promote quick, decisive response and remediation.
- Identify possible threats in ICS, IoT, and OT environments.
- Eliminate dangerous physical and virtual network blind spots.
- Receive continuous, automated threat detection and analysis in real time and retrospectively.
- Deploy OT security, with a choice of On-Premise or SaaS management and dashboard.
- Taps and Packet Brokers available in industrial grade, suitable for any OT environment.
About Nozomi Networks

Nozomi Networks accelerates digital transformation by protecting the world’s critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

www.nozominetworks.com