SOLUTION BRIEF

# Nozomi + Keysight: Visibility to Secure ICS and the Industrial Internet of Things (IIoT)

With the Internet of Things (IoT) bringing industrial operations online for the first time, network visibility and security must be extended to monitor and secure new devices. Nozomi Networks brings real-time visibility across Industrial Control System (ICS) environments 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.

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

### Highlights

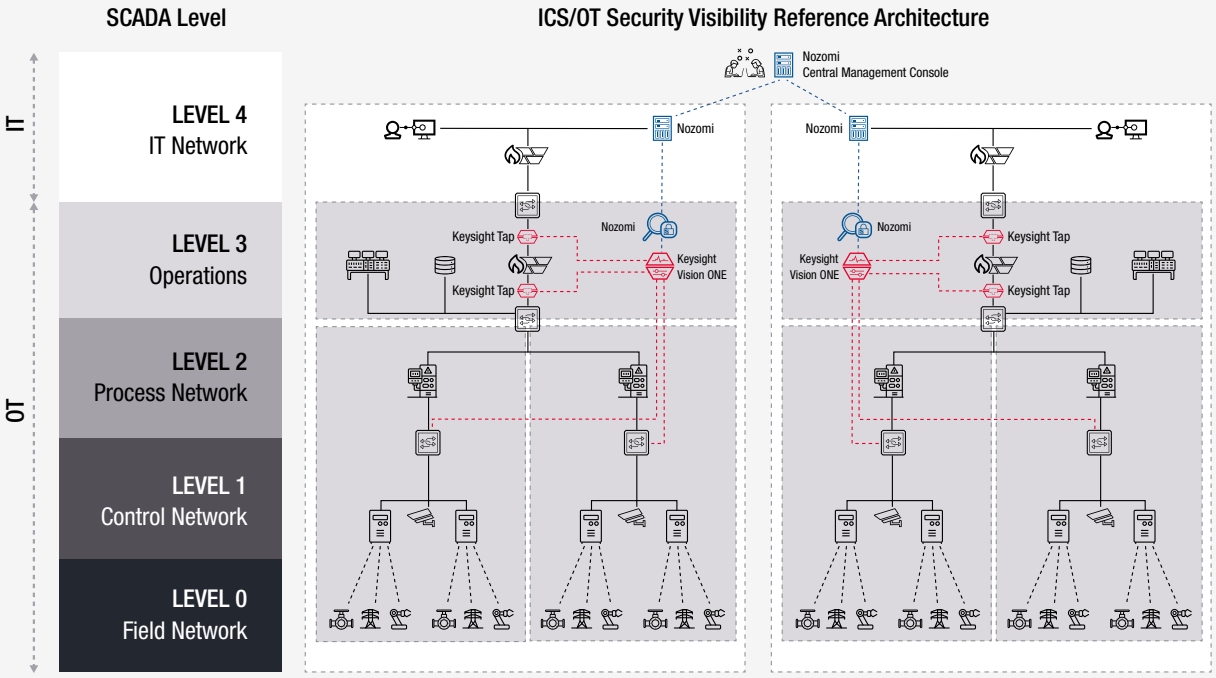
- Achieve real-time operational visibility
- Accelerate incident response (IR)
- Improve ICS cyber resiliency
- Save time and reduce effort
- Improve operational uptime

KEYSIGHT TECHNOLOGIES

# Nozomi: Best-in-class 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 take action to remediate cyber threats in real time.

The first ICS visibility solution powered by artificial intelligence (AI), Guardian offers nonintrusive visibility across ICS and SCADA (Supervisory Control and Data Acquisition) environments, including multiple geo-separated plants, without adding latency, determinism or jitter to the control network. Guardian delivers consolidated OT visibility, automatically learning all assets and working with your cybersecurity infrastructure to monitor networks and detect threats and anomalies.




**Detect, prioritize and resolve threats to ICS and IIoT infrastructures. With Nozomi and Keysight, data collection occurs across multiple levels in your ICS environment. Nozomi Guardian uses Keysight's visibility architecture to capture comprehensive data and eliminate network blind spots. Data gets consolidated onto a single Nozomi threat analytics platform to promote rapid incident response and proactive defense strategies.**

## Keysight: The Right Data for the Right Response

Keysight Network Visibility Solutions (NVS) deliver complete access to both OT and IT 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.

Tapping can be done in places where OT switches are not capable of adequately mirroring packets to ensure complete visibility. Taps may also substitute for data diodes since they allow copies of traffic to flow out of the monitored network segment but not back into it.

Data from the network gets forwarded to Keysight's Visions Network Packet Brokers (NPBs) for real-time processing and delivery to Nozomi Guardian. Pre-processing of traffic includes removing duplicate packets and stripping unwanted or privileged data to improve overhead and meet compliance mandates for securing information.

Vision NPBs aggregate, process, and deliver to Nozomi Guardian all relevant data from mirror and tap connections, filtering out traffic not relevant to SCADA security (such as CCTV video over IP traffic). The Vision series of packer brokers and Guardian can be integrated with security information and event management (SIEM) and other systems to establish automated threat response to indicators of compromise (IoCs). Keysight network visibility and Guardian also integrate with tools such as firewalls to improve policy enforcement and mitigate unwanted traffic.

**"The ICS security market is expected to reach $18 billion by 2023, driven by investments in Industry 4.0, convergence of Information Technology (IT) and OT, and a rise in the number of cyberthreats to critical infrastructure."**

**Markets and Markets**

## Joint Solution Highlights

Together, Nozomi and Keysight deliver comprehensive, highly automated visibility that helps defenders respond quickly, with confidence, every time. Highlights include:

- Detect attackers in real-time to promote quick, decisive response and remediation
- Identify possible threats in ICS, IIoT, and OT environments
- Eliminate dangerous blind spots
- Continuous, automated threat detection and analysis in real time and retrospectively

## About Nozomi Networks

Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. Leading the industry, we make it possible to tackle escalating cyber risks to operational networks. In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial sites around the world.

For more information, visit www.nozominetworks.com

## Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES