JOINT SOLUTION BRIEF

Provide Complete Visibility into Your Operational Technology Network to Improve Productivity, Minimize Downtime, and Secure Your Assets

Joint Solution Benefits

- Gigamon aggregates data from across the network to provide more visibility
- Nozomi catalogs operational technology assets across your network, analyzes its vulnerabilities, and baselines normal state to minimize downtime
- Nozomi provides anomaly detection of operational and security events with its unique AI and machine learning technology
- The Gigamon Visibility Fabric routes traffic and manages packets to optimize Nozomi's capabilities

The Challenge: Understanding and Securing Your OT Infrastructure

The distinction between information technology (IT) and operational technology (OT) is becoming blurred with industrial control and SCADA systems being connected to internal IT networks and the larger internet. Though this may increase efficiency, the interconnection increases the attack surface area of vital OT systems.

To better manage the risk of IT with OT integration, you need the right tools to access the relevant traffic in order to gain complete visibility to track and monitor assets, vulnerabilities, operational controls, and any abnormal changes. IT and OT tools need to work together to lock down your network, and intelligent network filtering and shaping capabilities are necessary to make sure network packets are delivered to the right place at the right time in order to truly protect your OT assets.

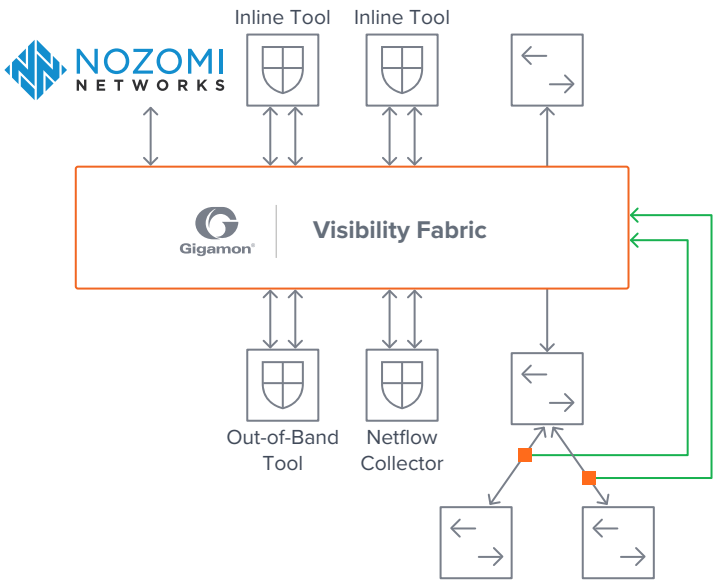
The Gigamon and Nozomi Joint Solution

Together, Gigamon Visibility Fabric™ and Nozomi Networks provide real-time network visualization and up-to-the-minute threat detection for your OT assets:

- Guardian™ protects industrial control networks from cyberattacks and operational disruption through passive network traffic analysis
- Smart Polling™ uses precise, low-volume active polling to provide a full OT asset inventory and vulnerability assessment
- The Central Management Console™ aggregates data for hundreds of distributed industrial installations, providing consolidated and remote access to your ICS data from Guardian appliances deployed in the field
- OT ThreatFeed™ has market leading threat detection of known and unknown threats. Its efficacy is further enhanced with Nozomi's AI and machine learning technology to detect anomalies.

The Gigamon Visibility Fabric combines with the Nozomi tools to offer comprehensive and integrated visibility across IT and OT assets. The Visibility Fabric enables traffic from across the network to be managed and delivered to Guardian and other tools efficiently and in the format they need, aggregates low-volume links together before forwarding them, de-duplicates packets to avoid unnecessary overhead, and offers easier control of asymmetric routing to ensure that session information is kept together for Nozomi's security tools to analyze.

The Visibility Fabric also provides load balancing, header stripping and masking for security and compliance. These features all allow the Nozomi solutions to automate the hard work of inventorying, visualizing and monitoring industrial control networks.



- Gigamon Visibility Platform can be used together with a multitude of other tools. Optimizing and filtering network traffic for all tools individually and concurrently
- Out-of-band Tools
  Tools like Nozomi Networks that requires a copy of network data and traffic to perform analytics, monitoring and reporting
- Netflow Tools
  Tools that require Netflow v5/v9/IPFIX to perform analytics, monitoring and reporting
- Inline Tools
  Flexible Inline Architecture with service chaining can be deployed with inline security tools such as NGFW and IPS, and/or Network Packet Shapers

For more information on Gigamon and Nozomi, visit:
www.gigamon.com and www.nozominetworks.com

Gigamon
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com