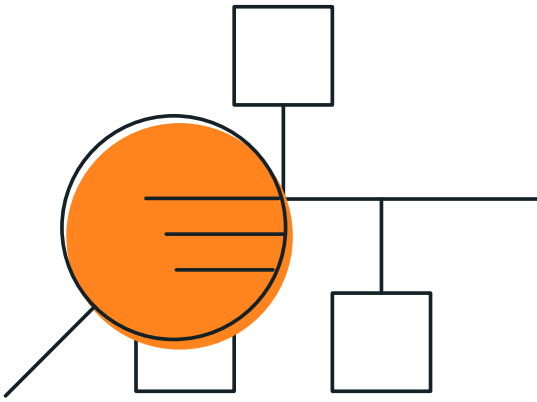
Gigamon® | NOZOMI NETWORKS

Get 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 comprehensive visibility
+ Nozomi Networks catalogs operational technology assets across your network, analyzes its vulnerabilities, and baselines normal state to minimize downtime
+ Nozomi Networks provides anomaly detection of operational and security events with its unique AI and machine-learning technology
+ The Gigamon Visibility and Analytics Fabric™ routes traffic and manages packets and flows to optimize Nozomi Networks' capabilities

The Challenge: Understanding and Securing Your OT Infrastructure

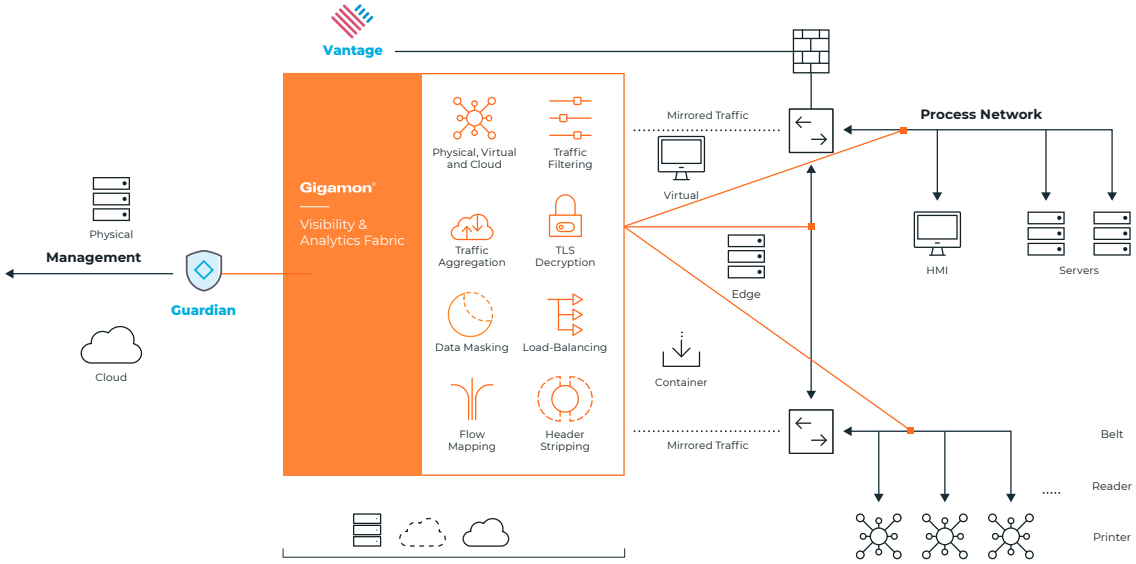
The distinction between information technology (IT) and operational technology (OT) is becoming blurred with industrial control and SCADA systems being connected to internal IT networks and the larger internet. Moreover, IoT devices are growing in vast numbers throughout many organizations. OT networks now include many IT machines and IoT devices like cameras, tablets, phones, badge-based access control units, and barcode readers. While pure-play devices like programable logic controllers (PLCs) are very different from IT, the different networks are converging very quickly. Though this convergence may increase efficiency, the interconnections increase the attack surface area of vital OT and IoT systems.

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

The Gigamon + Nozomi Networks Joint Solution

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

+ 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.
+ Threat Intelligence™ has market-leading threat detection of known and unknown threats. Its efficacy is further enhanced with Nozomi Networks AI and machine-learning technology to detect anomalies.
+ Asset Intelligence™ continuously updates Guardian sensors with rich OT and IoT device data so you can identify and respond to the most important security alerts faster.

The Gigamon VAF combines with Nozomi Networks tools to offer comprehensive and integrated visibility across IT and OT assets. The VAF enables traffic from across the network (physical, virtual, and cloud) to be managed and delivered to Guardian and other tools efficiently and in the format they need, aggregates multiple 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 Networks' security tools to analyze. Gigamon offers an optional unidirectional TAP capability to ensure OT production traffic is not negatively impacted and OT/IoT networks are not affected.

The Gigamon VAF also provides:

+ Load balancing to spread the volume of traffic across multiple instances of Nozomi Networks
+ Header stripping that makes Nozomi Networks tools more efficient
+ Masking for data privacy compliance
+ Optimization and filtering of network traffic sent to Guardian and other tools, individually and concurrently, by sitting between the production network (physical, virtual, cloud) and the Nozomi Networks platform and a multitude of other tools
+ Routing of relevant traffic to Nozomi Networks tools that require a copy of network traffic to perform analytics, monitoring, and reporting
+ Cost savings and improved ROI realized through centralized the Gigamon VAF de-duplicating packets, decrypting SSL/TLS flows, slicing packets or flows, filtering Layer 7 applications, and more

For more information on Gigamon and Nozomi Networks, 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