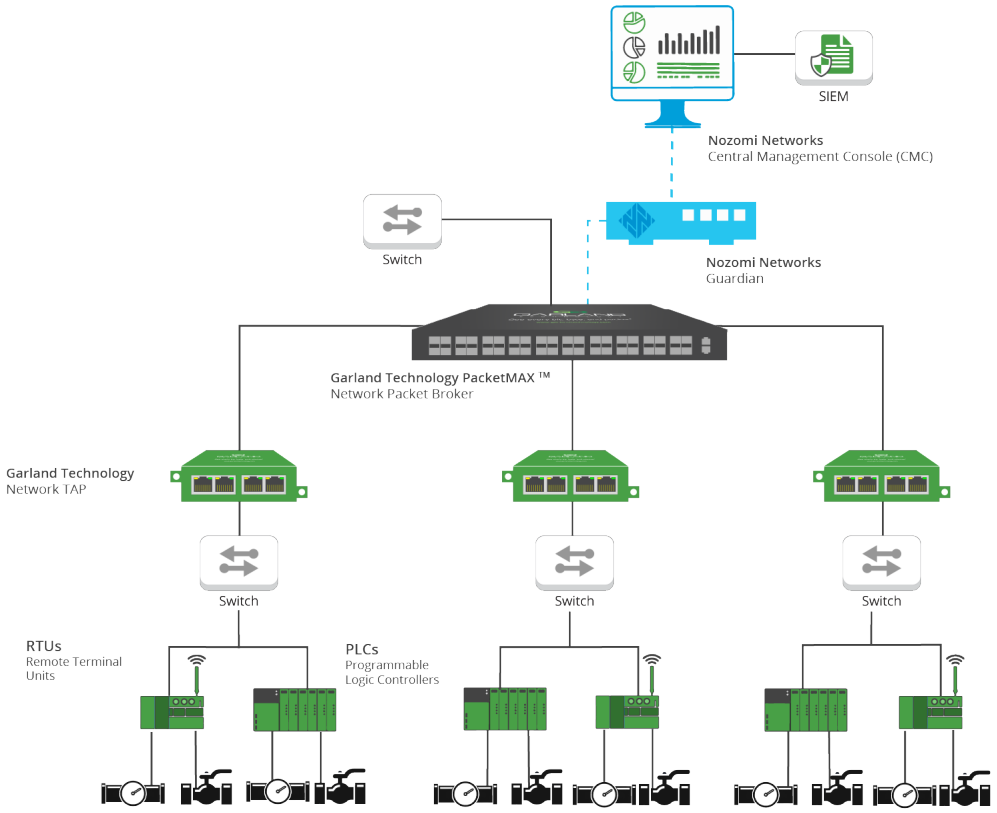
Unlock Visibility and Security Across OT, IoT, and IT Teams

Accelerated Security and Digital Transformation Across the Network

Until recently, operational technology (OT) networks were completely separated from information technology (IT) networks. This is quickly changing as industrial environments come online, expanding the attack surface for cyber threats beyond traditional IT assets. CISOs are now expected to manage and secure networks that span the entire organization, requiring operational visibility to include the wide variety of OT/IoT and IT devices on their networks.

Together, Nozomi Networks and Garland Technology enable complete visibility, control, and cyber resilience across your distributed network. Protecting your operation from threats and anomalies requires deep packet-level visibility and accurate, immediate information. The joint solution provides OT and IT teams the tools needed to obtain full visibility, significantly reducing the potential for disruption to production lines across the largest critical infrastructures in energy, manufacturing, mining, transportation, building automation, and other sites around the world.



How it works

1. Garland Network TAPs analyze data from substations and IoT- centric systems, mirroring the network traffic.
2. The Garland Technology TAPs allow multiple links to feed Garland's PacketMAX Advanced Aggregator, which combines, filters, and load balances the tapped traffic at scale into Nozomi Networks Guardian.
3. The Guardian analyzes the traffic to create a network map and identify vulnerable devices, cyber threats, and operational anomalies on your network.
4. The optional Nozomi Networks Central Management Console (CMC) aggregates data from all Guardian deployments to create centralized OT and IoT security management.

IT and OT Team Benefits

- Full-duplex copy of network traffic ensuring no dropped packets, passing physical errors, and supports jumbo frames.
- Provide 100% network visibility and data diode functionality without adding latency.
- TAPs do not have an IP address, or MAC address and cannot be hacked.
- Plug and play; easy configuration and deployment to improve reliability and reduce costs.
- Improve collaboration and break down silos across teams with deep visibility across all network and application layers and infrastructures.
- Catalogs OT and IoT assets across your network analyzes their vulnerabilities, and baselines normal state.
- Provides anomaly detection of operational and security events with its unique AI and machine learning technology.
- Combines behavior-based anomaly detection with signature-based threat detection for comprehensive risk monitoring.

Integration Benefits

The deployment of Nozomi Networks and Garland Technology provides visibility and security throughout your complex network. Garland collects data across on-premises and off-site locations, providing a centralized source of aggregated networking information. Nozomi Networks delivers network visualization, asset inventory, vulnerability assessment, and threat detection in a single application, making your OT and IT teams more effective. The joint solution enables you to quickly detect and respond faster to changes in your network, cyber threats, risks, and anomalies before they can disrupt operations.

About Nozomi Networks

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation, and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection, and operational insight.
www.nozominetworks.com

Learn More
GarlandTechnology.com/Nozomi

Let's Talk
+1 716.242.8500
sales@garlandtechnology.com

GARLAND TECHNOLOGY
See every bit, byte, and packet®