Radiflow

GARLAND TECHNOLOGY
See every bit, byte, and packet®

End-to-End OT Visibility and Cyber Protection

Protecting industrial networks by capturing every packet, delivering complete security visibility and real-time detection of anomalies

JOINT SOLUTION BENEFITS

- Ensures complete data capture of all network transactions, enabling effective anomaly detection
- Facilitates precise threat detection and reduces false positives through uninterrupted data analysis
- Maintains network performance and uptime with non-intrusive data streaming
- Adapts to a variety of network configurations and scales seamlessly with infrastructure changes
- Simplifies network management and security operations, enhancing overall control and visibility

Critical infrastructure and industrial operations rely on digital automation to increase productivity at scale. But operators of Cyber Physical Systems (CPS) face unique challenges when it comes to securing operations, data, networks, and devices. Today's automation systems host an array of vendors, legacy and modern assets, applications, and corporate IT systems, and are accessed by third-party integrators and consultants, increasing cyber exposure. Operators must carefully monitor their operations at all times to stay ahead of threats.

TAPS VS. SPAN

Two main technologies are used to monitor network traffic: Test Access Points (TAPs) and Switched Port Analyzer (SPAN) ports. While convenient, SPAN ports may not capture every packet, especially under high traffic conditions, leading to gaps in visibility and potential security risks. Furthermore, some switches do not support the SPAN protocol. TAPs provide an unaltered and complete view of network traffic, ensuring that every packet is accounted for.

In addition, TAPs are more secure since they are passive devices that cannot be accessed or tampered with through the network. Unlike SPAN, TAPs operate out-of-band and thus do not compete with operational network traffic; this is ideal for high-security environments as it enables separation of security monitoring from operational processes. TAPs may be used to extend visibility into additional parts of the network that don't support SPAN.

SEEING AND MONITORING EVERYTHING

Network TAPs are used mainly in networks without managed switches or with no SPAN capabilities. The joint solution creates security visibility in critical network with old, legacy, and low-resourced equipment. Garland Technology Network TAPs forward 100% of packets to the Radiflow iSID Threat Detection System deployed on-site. Providing a convenient industrial site-wide view, iSID maps and displays the network topology, including segments, devices, zones, and conduits. iSID's machine learning automatically establishes an accurate baseline of normal network and asset behavior and communications. It also allows operators to input and maintain operational and security policies and adds these to the baseline. As the TAPs deliver packets of traffic, iSID continuously monitors the network and promptly detects behavior and policy deviations that might be signs of cyberattack.

KNOWING YOUR ASSETS

With accurate traffic monitoring through the secure capture of 100% of packets, iSID continuously discovers and builds a complete inventory of legacy and modern assets while vigilantly protecting them to ensure safe, cyber-free operation. The always-up-to-date asset inventory may be uploaded to third-party asset management systems.

MANAGING ALERTS EFFICIENTLY

iSID alerts on behavior anomalies with rich context, enabling security analysts to respond rapidly either directly via iSID or through the SOC. iSID's alerts and playbooks can be shared with SIEM and other cyber solutions.

CYBER COMPLIANCE

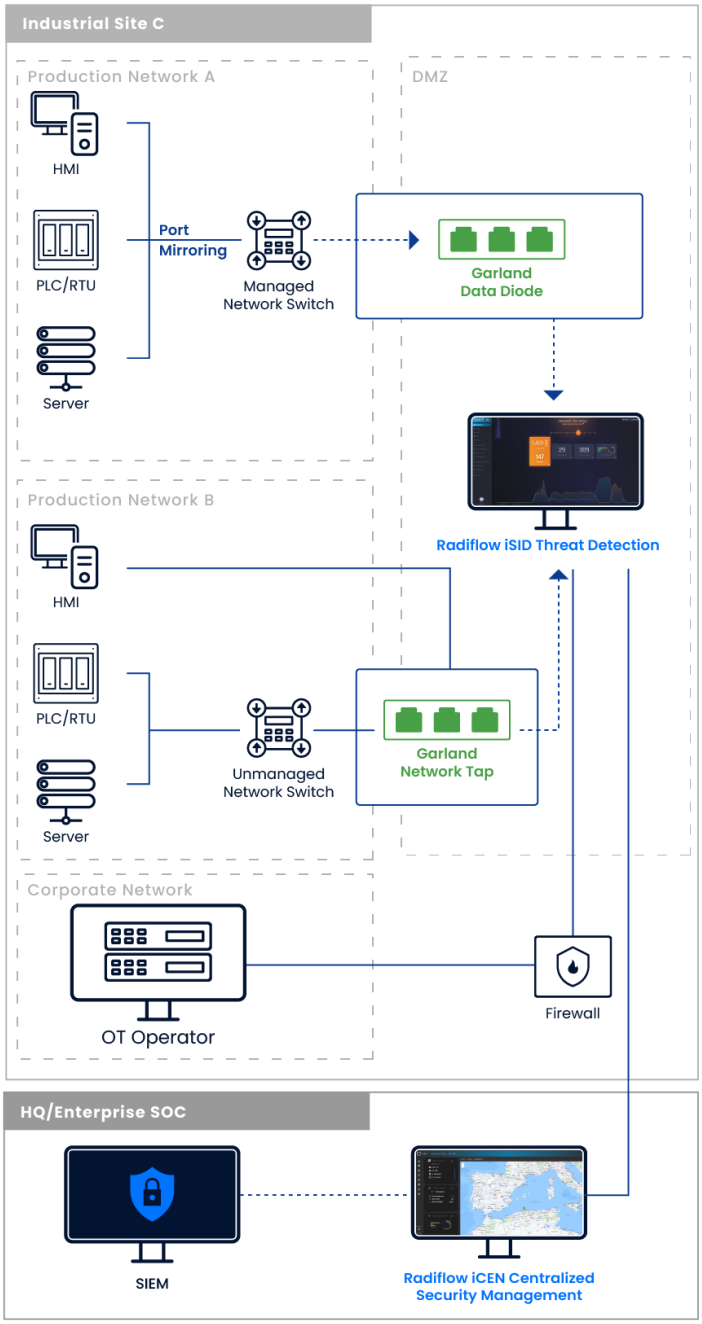
Many OT environments operate under strict regulations and standards that require detailed data logging and breach-detection capabilities. The combination of Radiflow and Garland Network TAPs helps ensure compliance with robust logging of all network traffic and advanced threat-detection capabilities.

FLEXIBLE, COST-EFFECTIVE DEPLOYMENT

The cost-effective Garland Network TAP allows up to 4 links to be tapped and aggregated together to feed the Radiflow iSID passively and out-of-band. Using a TAP instead of configuring a mirror port (SPAN) on a switch enables the delivery of unidirectional traffic via the built-in data diode of the TAP, guaranteeing safe delivery of 100% of the network packets.

CENTRAL CYBER MANAGEMENT OF MULTIPLE SITES

Radiflow iCEN simplifies and streamlines the monitoring and management of multiple instances of the Radiflow iSID Industrial Threat Detection System. From the iCEN, users are able to observe the status and activities of each iSID across the organization, obtaining a unified view of each site's cyber status with easy drill-down to detailed information. iCEN also enables single-click provisioning of up-to-date cyberattack detection signatures and user-defined rules to multiple iSIDs, enabling improved response time and detection of new threats across the organization. iCEN can share alerts and other information with the SIEM and other SOC solutions.



Radiflow develops OT Security and Risk Management solutions that ensure operational resilience and optimize cybersecurity expenditure. Radiflow's solutions enable local or centralized deployments, and integrate with leading technology-partner platforms. Now part of the Sabanci Group, Radiflow protects over 8,000 sites worldwide. Visit us at **www.radiflow.com**

GARLAND TECHNOLOGY
See every bit, byte, and packet®

Garland Technology is an industry leader of IT and OT network solutions for enterprise, critical infrastructures, and government agencies worldwide. Since 2011, Garland Technology has been engineering and manufacturing simple, reliable, and affordable Network TAPs and Network Packet Brokers in Richardson, Texas. For help identifying the right IT / OT network visibility solutions for projects large and small, visit **garlandtechnology.com**