PARTNER BRIEF

DRAGOS AND GARLAND TECHNOLOGY

Improving visibility across industrial networks and minimizing risk to legacy systems

HIGHLIGHTS

- Maximize performance powered by packet-level visibility for ICS/OT communications.
- Enhanced visibility and security throughout your environment, regardless of network complexity.
- Minimizing operational risk for legacy ICS/OT environments while supporting cybersecurity requirements.

THE CHALLENGE

Industrial control systems (ICS) are at the heart of our world's critical infrastructure, powering everything we enjoy in our connected society. While legacy ICS networks were designed primarily with reliability and safety in mind, evolving business objectives have triggered the supporting operational technology (OT) to keep pace over the past decade to meet these newer requirements. From power generation to manufacturing, food production to water and wastewater management, and pharmaceuticals, no industrial market has been immune to this digital transformation trend. However, even with these changes happening, the industrial asset operators must continue to ensure operations are running reliably, safely, and securely.

Unfortunately, not all ICS/OT environments can evolve simultaneously or have the capabilities to support the additional hardware and software needed to meet updated business and/or regulatory requirements. As organizations seek to centralize their views across all data sources to optimize operational efficiencies, legacy ICS/OT components not initially designed to be digitally secure now connect to expanding network infrastructures, adding more complexity. But without comprehensive visibility, OT cybersecurity teams have the nearly impossible task of attempting to secure these environments as digital transformation efforts are outpacing the cybersecurity protections. When it comes to defending industrial networks, organizations cannot afford blindspots, drop packets, or to suffer network downtime. In addition, some inherent challenges exist within legacy infrastructures where switches may not have port mirroring or switch port analyzer (SPAN) port options available or adequate system resources to utilize them. Or, in more modern ICS/OT environments where the SPAN ports and resources are available on the switches, they can be prone to drop packets, send unnecessary duplications, or may already be reserved for another purpose.

THE SOLUTION

The need for passive, real-time monitoring is more vital than ever in an ICS/OT environment saddled with legacy equipment. Passive network TAPs (test access points) are purpose-built hardware devices that provide essential access and monitoring capabilities in ICS/OT environments. Passive network TAPs are available in fiber and 10/100M/1000M copper models. By tapping points of interest throughout the ICS/OT network, security and other monitoring solutions can receive 100% of the traffic to enhance their defense capabilities without introducing new or manipulated traffic to the production network streams.

Garland's Aggregator TAPs are used to capture 100% full-duplex traffic and then send it to multiple monitoring appliances for network analysis. Aggregator TAPs supports aggregation and regeneration/SPAN modes, as well as tap 'breakout' mode, providing flexibility to manage your network. Garland's unique design provides a unidirectional path to the monitoring ports of the Aggregator TAP, ensuring that no Ethernet packets can be sent to the live network TAP or SPAN ports.

As the saying goes, 'You cannot secure, what you can't see', organizations cannot effectively protect the OT assets they do not know about. Therefore, visibility of the ICS/OT network is both the tactical and strategic foundation of an effective cybersecurity program. Organizations can leverage Garland's visibility solutions to feed data to the Dragos Platform to help streamline the security of the ICS/OT network infrastructures while helping to avoid operational impacts in legacy systems. Utilizing this network and other host-based data, the Dragos Platform allows users to visualize the systems, devices, and their interactive communications, detect threats as they occur, and utilize prescriptive workbench tools for more efficient investigations and response.

To truly understand the actual cybersecurity risk for the ICS/OT environment, organizations must ensure that the aperture of their asset visibility lens includes primary, secondary, and tertiary devices and how their systems are communicating to and throughout the infrastructure. To do that, you need purpose-built solutions that can provide 100% access to the relevant traffic in ICS/OT environments where legacy and distributed networks present unique challenges. By utilizing the joint Garland and Dragos solution, organizations gain continuous visibility into their ICS/OT environments to efficiently and effectively track and monitor assets, vulnerabilities, operational controls, and any abnormal changes. With this enhanced deep packet level of visibility across critical infrastructures, defenders can more competently protect their operations from potential disruption caused by threats and anomalies while improving their safety, reliability, and cyber resilience across their unique network infrastructures.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
More effective network visualization and efficient security operations	Aggregation of data for distributed ICS/OT environments to quickly detect and respond faster to changes in the network, cyber threats, and anomalies before they can disrupt operations.
Enhanced visibility of ICS/OT networks regardless of complexity	Clear the path towards digital transformation within legacy environments by delivering the critical insights needed to defend your ICS/OT assets against undetected failures and costly outages.
Create more secure architectures in ICS/OT networks	The joint architecture reduces blind spots, allowing for the safe monitoring of industrial networks for enhanced asset identification and threat detection.
Full-duplex copy of network traffic in a simple deployment without adding complexity or significant costs	Plug and play style deployment with easy configuration options provide 100% network visibility and unidirectional capabilities for security monitoring without adding latency, vulnerabilities, or sacrificing reliability.

For more information, please visit www.dragos.com or contact us at info@dragos.com