Darktrace + Garland Joint Solution

OT Network Visibility for Complex Industrial Environments

DARKTRACE

Security Challenges

Increasing convergence of IT and OT environments has expanded the attack surface and introduced new security risks for critical infrastructure. Older and inherently vulnerable Industrial Control Systems (ICS) that were previously 'air gapped' or isolated are becoming increasingly exposed to threats as IT and OT converge. Additionally, as the number of industrial IoT devices has risen dramatically over the past several years, the overall level of visibility for security teams into these assets has decreased, creating easy entry points for attackers.

OT security teams continue to suffer from a growing skills shortage, tight budgets, and are understaffed compared to the IT security teams. Furthermore, as United States and European regulations on OT/ICS tighten, critical infrastructures must find a way to improve their OT security posture with an easy to deploy solution providing visibility across all Purdue Levels.

Darktrace/OT + Garland Technology

With its unified view of IT and OT environments, Darktrace is uniquely positioned to deal with relevant threats to IT/OT and the challenges posed by convergence and segmentation.

Darktrace/OT detects and responds to attacks in their earliest stages before costly damage is done. Darktrace/OT uses raw network traffic from an OT network to understand the normal pattern of life for every device and operator in the industrial environment. If a human or machine displays even the most nuanced forms of threatening behavior, the solution can identify this in real time based on statistical anomaly score.

Darktrace/OT does not need any data or threat feeds from external sources because the AI driven software builds an innate understanding of self without any need for third-party support or data. All data processing and analytics are performed locally on the Darktrace appliance. With no connection to the Internet required, Darktrace/OT functions within air-gapped or highly segmented networks without jeopardizing their integrity.

Garland Technology's Network TAP and Packet Broker solutions enable the seamless deployment of Darktrace appliances in any OT environment. With the built-in data diode technology of many of the Garland TAPs and Aggregators, organizations are able to guarantee complete network visibility and have confidence that network traffic is unidirectional.

GARLAND TECHNOLOGY

See every bit, byte, and packet®

About Garland Technology

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, Aggregators, Network Packet Brokers, and Data Diodes in Richardson, Texas.

To learn more about Garland Technology, visit GarlandTechnology.com.

Key Solution Benefits

- Increased visibility across OT, IT, and IioT to Purdue level 1 where there is lacking existing switching infrastructure.
- Protocol and technology agnostic
- Illuminates points of IT/OT convergence.
- Reduces risk of misconfigured switch ports.
- Guarantees unidirectional traffic flow with data diode protection.
- Reduce complexity of deployment in distributed networks.
- TAPS do not have an IP or MAC address so are not hackable from a network standpoint.
- Zero hardware subscription fees from Garland Technology.

DEPLOYMENT OPTIONS

Scenario 1: Network TAP

When a customer does not have access to layer 3 switching or does not want to configure a SPAN or Mirror port to deploy Darktrace/OT, a Network TAP can be utilized. In a simple deployment architecture, a Garland Technology Network TAP will pass all network traffic from the tapped network link to the Darktrace appliance. With the hardware data diode design of the Garland Network TAP, this solution guarantees unidirectional traffic flow.

Scenario 2: SPAN Aggregation

When a customer wishes to use a configured SPAN/Mirror port on the Switch as the access method for Darktrace and is looking to capture mirrored traffic from multiple SPAN links, a Garland Aggregator TAP can be used to deploy the Darktrace appliance. With the hardware data diode design of the Garland Network TAP, this solution guarantees unidirectional traffic flow, while aggregating up to 8 SPAN/Mirror ports to 1 or 2 Darktrace appliances.

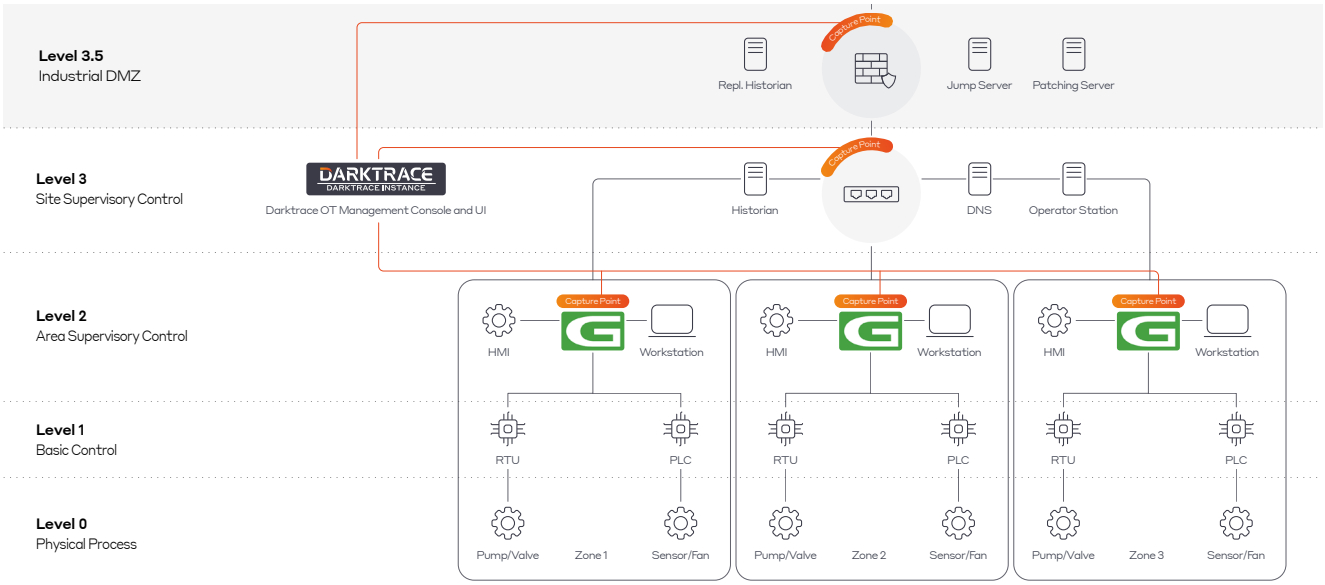

Figure 1: Where switching infrastructure may not exist or support port mirroring Garland taps can be used to facilitate Darktrace's passive traffic analysis

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted in over 145 patent applications filed. Darktrace employs over 2,200 people around the world and protects c.8,800 organizations globally from advanced cyber-threats.

Scan to LEARN MORE