SOLUTION BRIEF

Comprehensive Security Operations for Any OT Environment

GARLAND TECHNOLOGY

See every bit, byte, and packet®

STELLAR CYBER®

With the convergence of Operational Technology (OT) and Information Technology (IT), securing all environments from cyber threats efficiently and effectively has never been more critical. Securing and defending OT environments has historically been challenging due to the inability to deploy agent-based solutions, uncommon protocols, managed or legacy switches, and unidirectional connectivity requirements.

Stellar Cyber and Garland Technology partner to deliver a joint technical solution that allows enterprises to realize the right OT security program, regardless of data sources or network requirements, and remove that legacy challenge. Stellar Cyber delivers a Security Operations Platform built on Open XDR and sensors natively supporting OT. Garland Technology provides Network TAP solutions guaranteeing complete packet visibility in any environment. Together, enterprises can get immediate security results and future-proof their security program.

STELLAR CYBER®

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Open XDR Platform

- Ingests, normalizes, and enriches all your security data, including OT, endpoints, network, cloud, and logs into a single repository, replacing legacy SIEMs
- Automatically detects and correlates alerts using a proprietary multi-modal threat detection engine driven by machine learning
- Collects and detects in edge environments, including OT, with multi-function network security sensors
- Provides automated and manual response actions in real-time

Network Visibility

- Provides 100% complete network visibility through Network TAPs (Test Access Points) without affecting network traffic
- Optimize network monitoring through purpose-built Packet Brokers that allow advanced aggregation, filtering, load balancing, and deduplication
- Delivers inline Bypass TAPs to manage new inline tool deployments without disrupting operations
- Utilizes Data Diodes to segment network environments with unidirectional constraints
- Deployable solutions in specialized environments (e.g. OT) and in any form factor (hardware vs. virtual)

Benefits

- Enhanced visibility reduces the risk of damaging breach
- Dramatic increase in security analysts' productivity and efficiency
- Reduce attacker dwell time, minimizing attack impact
- Improve ROI of your existing security stack investment in IT and OT

Benefits

- Complete visibility regardless of the network architecture constraints
- Future proofed network monitoring to scale up to any speeds or changes in underlying infrastructure
- Reduce overall cost of network monitoring through complete portfolio of TAP and Packet Broker products
- Zero hardware subscription fees

Joint Approach To Defending OT

Stellar Cyber's role in defending OT environments is to get telemetry from every relevant system, deploy its sensors for NDR and other network-based detections in relevant environments, and perform automated threat detection to power the security operations program. Garland Technology's role in defending OT environments is to provide packet-level visibility, no matter the network architecture constraints, and provide unidirectional network segmentation.

The objective of deploying Stellar Cyber and Garland Technology is to get complete, cost-effective visibility which will ultimately deliver the best security outcomes. Both companies offer flexibility on specific products or components deployed depending on the deployment scenario. Use the below deployment matrix to understand how to deploy to defend your OT environment optimally.

The deployment scenarios below reference the Purdue Model for Industrial Control Systems.

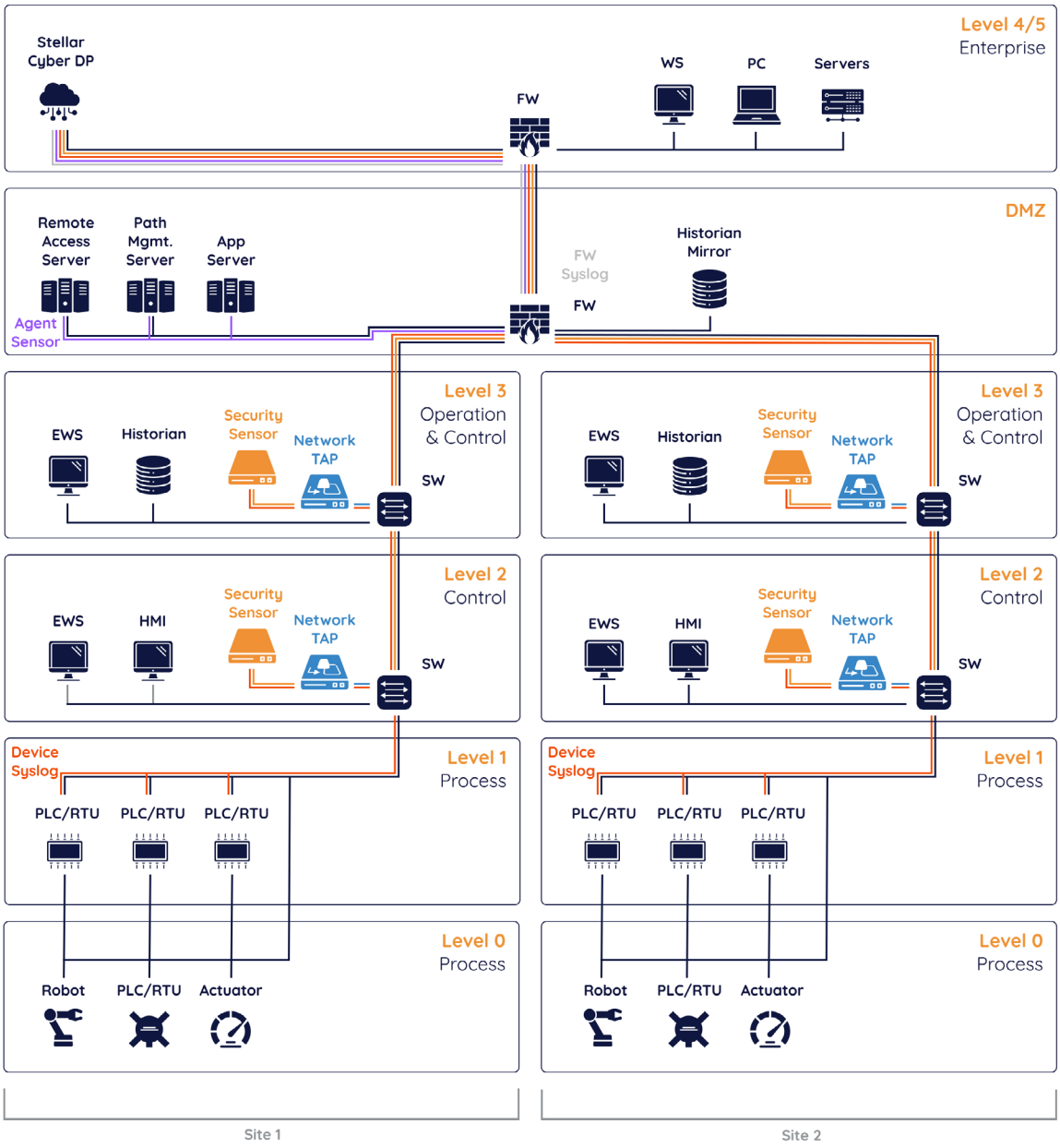
Deployment Scenario	Stellar Cyber Architecture	Garland Technology Architecture
1. Agentless network Security Sensors allowed in Level 3 and Level 2	• Security Sensors deployed in Level 3 and Level 2 off of core switches • OT syslog collected directly to Security Sensors	• TAPs optional depending on physical network requirements (media type/speed)
2. Agentless network Security Sensors NOT allowed in Level 3 and Level 2	• Security Sensors deployed in Level 4 off of packet broker • OT syslog collected via syslog server sending telemetry to Level 4	• Packet Broker deployed in Level 3 • Aggregator TAPs deployed in Level 2 sending traffic to Packet Broker • Data Diode optional depending on unidirectional requirements
3. Require unidirectional connectivity between Level 4 and Level 3 environments	• Security sensors in Level 3 and below must be manually updated	• Data Diode deployed between Level 3 and Level 4
4. Legacy or unmanaged switches	• Security Sensors deployed in Level 3 and Level 2 off of Network TAPs, if allowed • Otherwise, Network TAPs feed Packet Broker, which then feeds Security Sensors	• Network TAPs deployed to mirror switch traffic to Security Sensors
5. DMZ hosts allow agents for security	• Agent Sensors deployed on DMZ hosts for telemetry collection	*Does not affect architecture*

Example Deployment – Multi-Site Complete Visibility

If an enterprise had no restrictions on what security and networking solutions could be deployed in Level 3 and Level 2, and wanted to optimize for complete visibility, they would opt for an architecture similar to below. In this architecture, Network TAPs are deployed on each switch in Level 3 and Level 2 because of potential limitations with natively capturing SPAN traffic. Additionally, using TAPs in this deployment will ensure the customer gets visibility into both north-south traffic and east-west traffic.

Without the use of TAPs, customers are unable to gain visibility into their east-west traffic. Security Sensors are attached to each Network TAP and send all telemetry and detections back to a central Stellar Cyber Data Processor. Security Sensors deployed in Level 3 and below allow for active scanning, such as Vulnerability Management and easy telemetry collection.

This example architecture is deployed at multiple sites (e.g. Local Plants, Waste Treatment Facilities, etc.) for complete enterprise coverage. Other security telemetry is collected when possible.

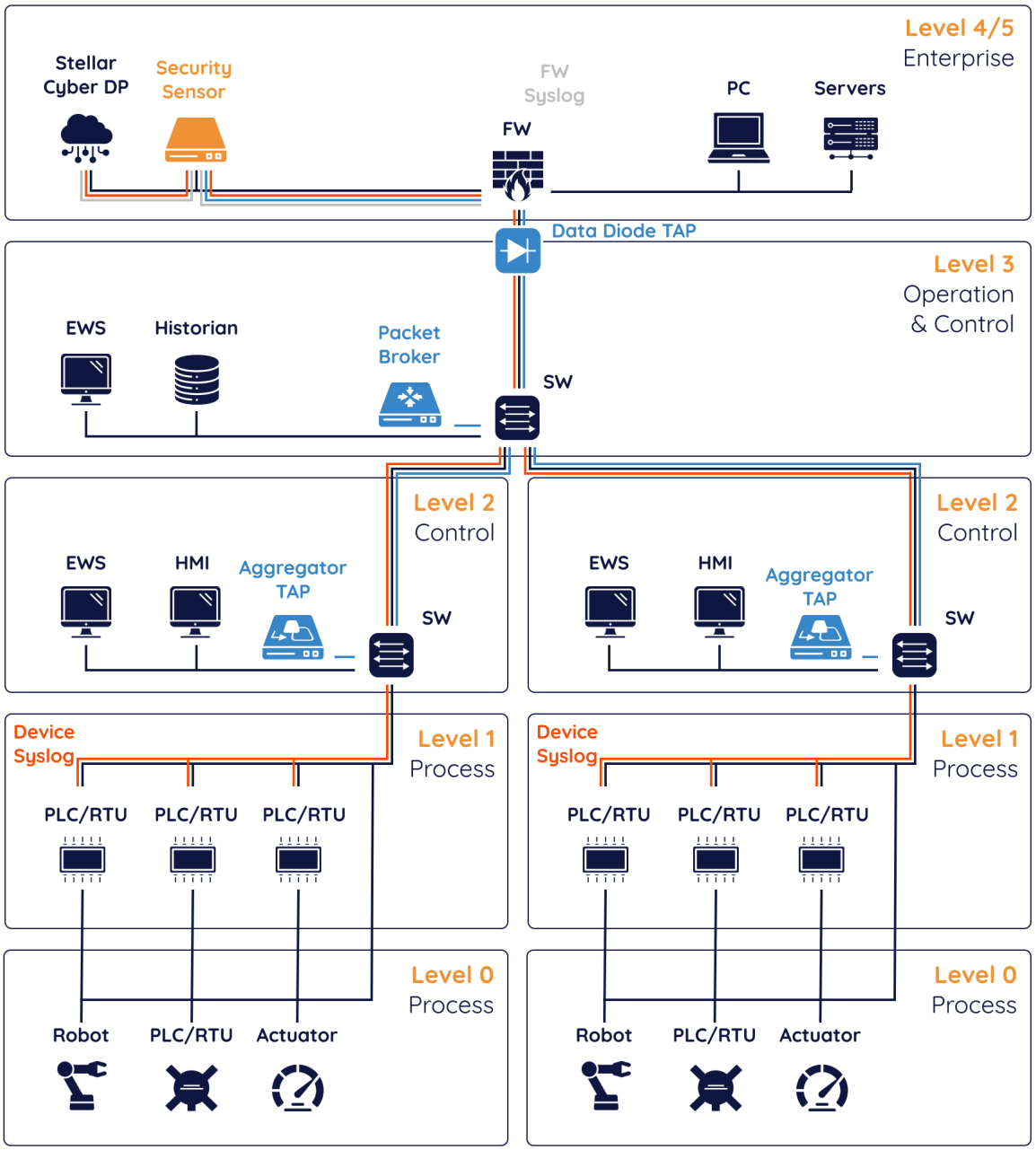


Example deployment prioritizing complete visibility and getting Security Sensors into Level 3 and below. This example architecture has a DMZ between Level 4 and Level 3, with no Data Diode in between.

Example Deployment – Packet Aggregation Through Data Diode

If an enterprise has limitations on what security solutions could be deployed in Level 3 and Level 3, yet still wants to get network level security detections and OT telemetry out of the OT environment, they would opt for an architecture similar to the below. In this architecture, Aggregator TAPs mirror all traffic from OT switches and send it to a centralized Packet Broker. This Packet Broker then forwards the aggregated traffic from a Data Diode TAP to a Security Sensor positioned in Level 4. The benefit of this architecture is that it is less risky to accept in the OT network, there is still solid visibility, and Security Sensors can be automatically updated from the central Data Processor.

This example architecture is deployed only at a single OT site but could easily be replicated across multi-site environments. Other security telemetry is collected when possible.



Example deployment prioritizing a low-risk approach to getting network security and OT telemetry from the OT environment without placing security sensors in Level 3 and below. This example architecture has a unidirectional Data Diode between Level 4 and Level 3 and no DMZ.

Take the First Step Today

Every security team should be able to deliver continuous, consistent security regardless of their skills or experience. With Stellar Cyber Open XDR and Garland Technology, you get the capabilities to protect your corporate and OT environments fast. Visit stellarcyber.ai and garlandtechnology.com for more information.

stellarcyber.ai

garlandtechnology.com

Stellar Cyber Open XDR platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering a 20X improvement in MTTD and an 8X improvement in MTTR. The company is based in Silicon Valley. For more information, contact www.stellarcyber.ai.

STELLAR CYBER®

www.stellarcyber.ai | sales@stellarcyber.ai