GARLAND TECHNOLOGY
See every bit, byte, and packet®

+ MICROSEC

Detect and Eliminate Zero Day Attacks at the Edge

Secure the Edge for Industrial IoT and OT Systems with MicroSec & Garland Technology.

Sprawling industrial networks can be challenging to manage and protect. With critical assets deployed across plants, factory floors, and substations, security teams have the difficult task of ensuring their organization is protected from cyber attacks. That's why it's vital for security teams to develop a robust security posture, focused on the entire network, especially the Edge.

Designed for brownfield environments, MicroSec secures the Edge for Industrial IoT and OT systems with MicroSec's MicroIDS Monitoring Suite solution. First of its kind, MicroIDS users benefit from passive, continuous monitoring for vulnerabilities and threats in their industrial network from level 0 to level 4 for both IP/Ethernet and non-IP/non-Ethernet networks. MicroIDS is an ultra lightweight intrusion and tamper detection system utilizing advanced machine learning models to instantly detect Zero-Day attacks and known threats at both the field device and network level. In order for customers to realize full visibility of their network devices, MicroIDS must receive network traffic. Which is why MicroSec chooses Garland Technology. Garland Technology Network TAPs, Data Diode, and Packet Broker solutions provide MicroIDS with a complete copy of the network traffic, no matter what the network environment looks like or where the traffic is coming from.

Benefits of MicroSec

- Instantly detect and isolate threats, anomalies, and vulnerabilities on field devices and OT networks
- Monitor across IP/Ethernet and non-IP/non-Ethernet based networks to maximize coverage
- Detect, map and manage all devices across your network from level 0 to level 4
- Uncover untrusted and unknown devices as well as malicious data traffic on your network
- Root cause detection of compromised devices, stopping attacks before they spread
- Automatically mitigate and remediate attacks, threats and vulnerabilities

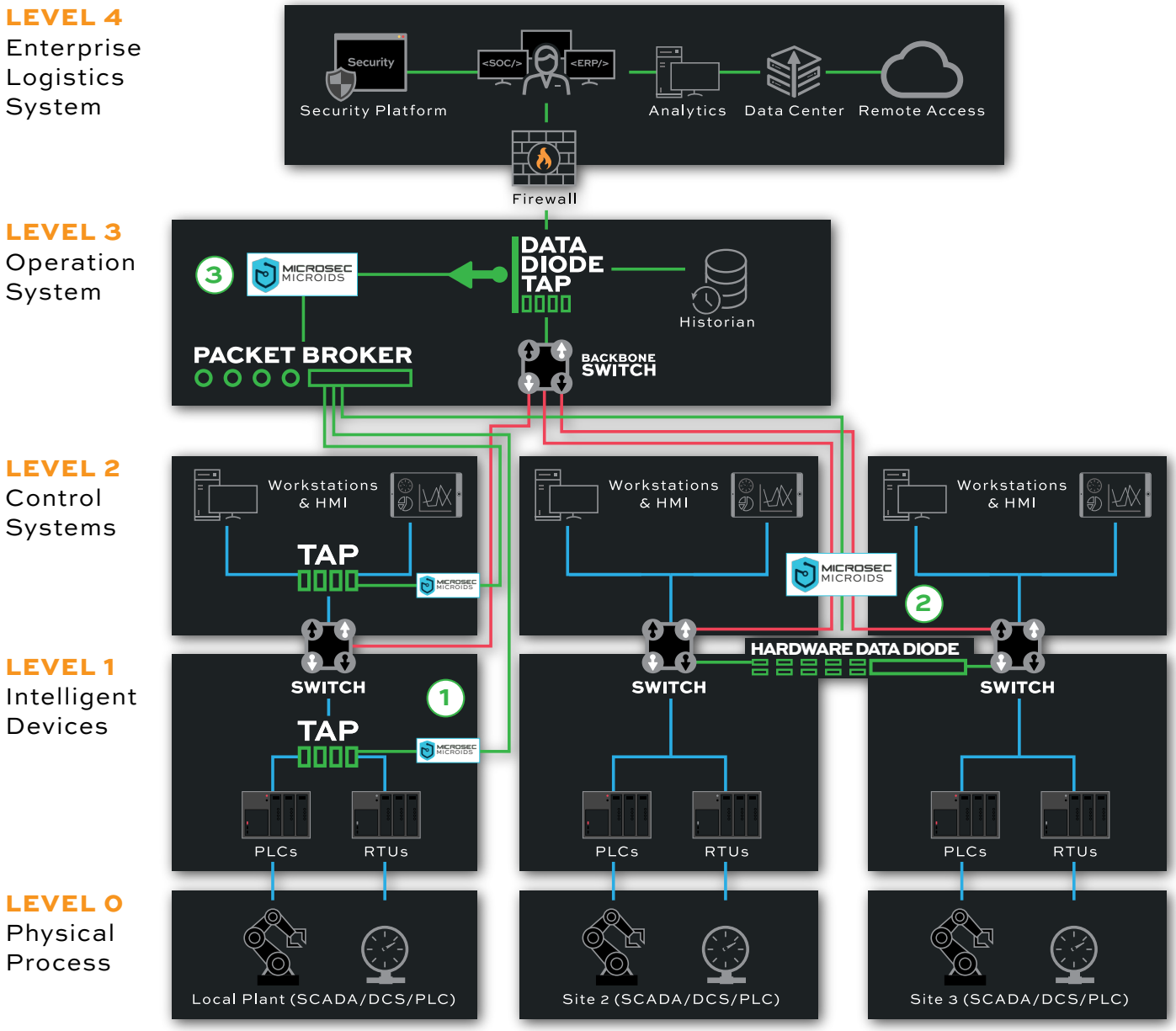
In order for customers to realize full visibility of their network devices, MicroIDS must receive network traffic. Which is why MicroSec chooses Garland Technology.

Benefits of Garland Technology

- Guarantee 100% full duplex network traffic with no packet loss
- Ensure unidirectional traffic flow with Data Diodes
- Products engineered for extreme OT environments including heat and vibration
- Maintain network integrity for industrial network monitoring without exposing additional risk
- 100% secure and invisible - Network TAPs have no IP address, no MAC address
- Enable deployment of security tools when switch ports aren't available

Three ways to deploy MicroSec MicroIDS with Garland Technology

1. MicroIDS connects to individual switches via a Hardware Data Diode
2. MicroIDS connects to TAP Aggregator
3. MicroIDS connects to TAP Packet Broker



Ways to Deploy MicroIDS with Garland

When a SPAN port is available on the switch, customers may prefer to use this route to deploy the MicroIDS since it will allow for a base level of visibility and protection right away. This application has its advantages because it will be a quick and fast deployment. However, there are security risks associated with using the SPAN port on a switch, so customers may deploy a Garland Hardware Data Diode to ensure unidirectional traffic to the MicroIDS, guaranteeing the SPAN port doesn't become a point of entry into their network.

A more robust solution includes the use of Network TAPs to send traffic to the MicroIDS. This approach provides a higher level of security as a customer is not relying on the correct configuration of a switch into a SPAN port to send copies of traffic to the MicroIDS. Deploying Network TAPs ensure more traffic and thus more assets are sent to the MicroSec appliance for analysis and protection. Also, there is the added benefit of the unidirectional protection of the Data Diode in the Network TAP itself when deployed.

Customers who are looking for visibility into multiple links in a network can also use a Garland Network Packet Broker to aggregate the different links, filter out traffic, such as camera traffic, that MicroSec does not need to see, before sending the groomed traffic to the appliance. This approach ensures that the sensor isn't overburdened or processing unimportant information.

About MicroSec

Launched in 2016, MicroSec is the first in the world to achieve Security-by-Design for constrained IoT devices, and is a global market leader in IoT security for OT environments, enabling end-to-end security from the Edge. MicroSec's industry expertise includes critical infrastructure, industry 4.0, energy, smart cities, and automotive, securing from level 0/1 to the cloud and on-prem. Please visit us at www.usec.io or contact us at info@usec.io for more information on our complete Edge security and monitoring solutions.

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 and Network Packet Brokers in Richardson, Texas. For help identifying the right IT / OT network visibility solutions for projects large and small, or to learn more about the inventor of the first bypass technology, visit GarlandTechnology.com.

Have Questions?
sales@garlandtechnology.com | +1 716.242.8500
GarlandTechnology.com/microsec

See every bit, byte, and packet®

10.17.23