

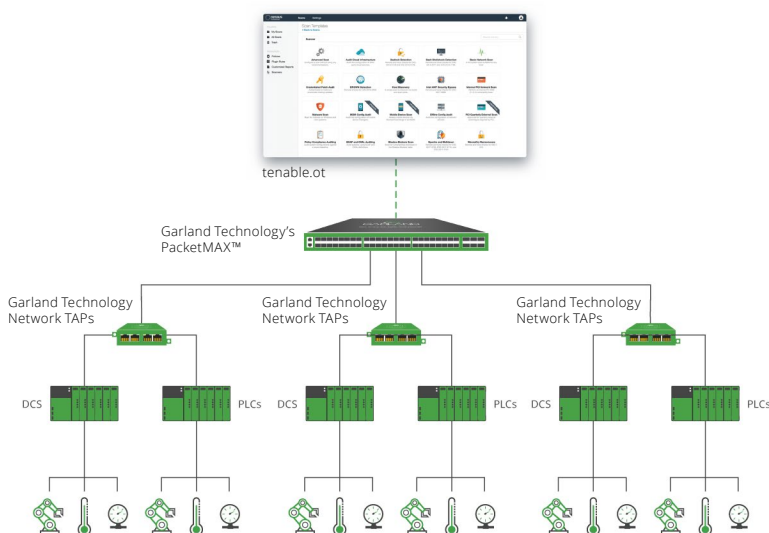


Identifying Vulnerable Traffic In OT and IT Environments

Eliminating Blind Spots And Continuous Monitoring Across Critical Infrastructures

Billions of IoT devices equal massive disruption. As new connected devices populate modern plants and factories they provide major disruption to OT infrastructures and make them increasingly vulnerable to cyber threats. Without comprehensive OT security, your attack surface and attack vectors increase, leading to unacceptable risk. Laying the proper network connectivity architecture to incorporate these ICS security solutions rely on one fundamental foundation concept — 360 degree visibility. And all of that starts with the packet.

By gaining complete packet-level visibility, networks can ensure continuous monitoring by detecting vulnerabilities in potential blind spots. As infrastructures continue to conduct digital transformations introducing IoT and smart technology, these files become increasingly difficult to detect and require continuous non-intrusive monitoring. Tenable and Garland effectively eliminate blind spots which can harbor lateral threats that can traverse IT and OT. Together we deliver a full stream of traffic for complete coverage of your modern attack surface, unifying your OT and IT security that detects threats early and proactively addresses vulnerabilities. Without complete visibility, security and control across the converged IT and OT, the likelihood of getting attacked is not a matter of 'if'; it's a matter of 'when.'



HOW IT WORKS

1. Intelligent network visibility starts by using physical and virtual TAPs to copy full-duplex traffic from any IT and/or OT network at each layer and site. Garland's network TAPs help overcome limitations that occur when SPAN Ports (switched port analyzer) are used, providing complete network visibility from each Distributed Control Systems (DCS), Programmable Logic control unit (PLCs), or segment that needs monitoring.
2. To optimize the network traffic, the tapped data is delivered from each station to Garland Technology's PacketMAX™ for aggregation, load-balancing, and filtering.
3. Once aggregated, the packet-level data feeds tenable.ot for efficient and continuous monitoring.

Integration Benefits

By capturing and sending packet traffic from anywhere in the network, Garland Technology is able to provide complete visibility across the entire network. Tenable.ot is then able to gain full visibility for deep packet inspection, helping to unify OT and IT security teams. The security solution provides unidirectional connectivity with diode functionality and streamlined network complexity through traffic aggregation. By eliminating OT and IT blind spots and reducing network complexity, Garland Technology and Tenable.ot provides an integrated passive monitoring solution to manage your entire ecosystem.

IT and Security Operations Benefits

- Full-duplex copy of network traffic ensuring no dropped packets.
- Provide 100% network visibility with unidirectional data diode functionality across converged IT/OT operations, eliminating blind spots that can harbor lateral threats.
- Gain full visibility across converged IT/OT operations. Detect and mitigate threats that impact industrial and critical operations by leveraging multiple detection methodologies.
- Identify and track IT and OT assets. Gain deep knowledge and situational awareness into the operation and state.
- Reduce risk by identifying vulnerabilities and potential threats before they become exploits and impact industrial operations.
- Track configuration changes with full audit trail capabilities.
- Determine whom, what and why changes were made as well as the result of those changes.
- Accommodate extreme OT environments with rugged TAPs, DIN rail, DC power converters, various secure connector options.
- Visibility with Zero IP address or MAC address and therefore cannot be hacked.
- Plug and play network TAP visibility; easy configuration and deployment to improve reliability and reduce costs.

About Tenable

Tenable®, Inc. is a Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com

About Garland Technology

Garland Technology is a trusted leader in critical infrastructure visibility solutions for OT, enterprise, service providers, and government agencies worldwide. We believe secure network visibility should be an easy, seamless experience. Since 2011, Garland Technology has worked with OT customers to identify their unique challenges and requirements for critical infrastructure environments and deliver the industry's most reliable Network TAP, Data Diode, Network Packet Broker and cloud visibility solutions, that deliver packet visibility while ensuring the secure connectivity needed. Find your solution at GarlandTechnology.com

[Learn More](#)

GarlandTechnology.com/tenable

[Let's Talk](#)

+1 716.242.8500

sales@garlandtechnology.com

