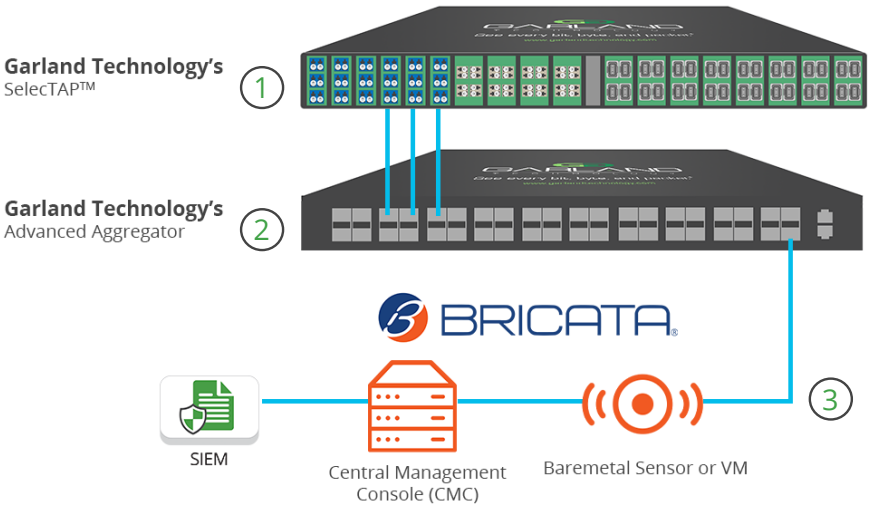
Bringing A Proactive and Responsive Approach to Unseen Network Threats

Detect and Defend With AI-Based Malware Conviction and Anomaly Detection

With the combined growth of network-driven business demands and the evolving complexity of cyber threats, organizations require network-level threat hunting to defend their business initiatives. When moving critical data across the network, they are often left open to unseen hackers or anomalies in blind spots without the proper range of security tools.

Bricata and Garland have teamed up to provide 100% visibility with a proactive approach to threats. Distributing data across increased capacity demands, the solution defends against network threats with signature inspection, anomaly detection, and AI-based malware conviction. The solution exposes alerts and malicious activities with complete context, providing traffic metadata all the way down to PCAP, increasing productivity, reducing time to containment, and minimizing operational costs.



How it works

1. Garland's high-density SelectTAP™, which accommodates 16 to 24 network TAP modules based on configuration, provides 100% packet acquisition where packets are recorded.
2. The mirrored packet-level traffic is delivered to the Garland Technology PacketMAX™ Advanced Aggregator, where the data is load-balanced and filtered. The aggregation layer eliminates oversubscription and provides optimal performance throughout the network.
3. The traffic enters the Bricata platform allowing comprehensive network threat detection for business data inspection.

IT Operations and Sec Ops Team Benefits

- Reliable zero-loss packet processing.
- A single platform to proactively hunt the network for threats as well as analyze alerts and respond.
- Provides enterprise-wide visibility and remote location defense.
- Automated threat detection based on signatures, stateful anomalies, and AI-based file assessments.
- Delivers alerts with context (leverages enriched network metadata).
- Reduced time to containment.
- Installation is done on premises with collected traffic never needing to leave the network.

Integration Benefits

With 100% packet acquisition and delivery through the Garland Technology visibility portfolio, Bricata's intuitive platform transitions packets from both known and unknown malicious activity. Whether on premises, multilocational, or virtual, this flexible deployment eliminates any possible bandwidth issues by removing unnecessary packets and filtration before forwarding traffic, allowing optimal threat detection and performance from the Bricata platform.

About Garland Technology

Garland Technology is an industry leader delivering network products and solutions for enterprise, service providers, and government agencies worldwide. Since 2011, Garland Technology has developed the industry's most reliable test access points (TAPs) and packet brokers, enabling data centers to address IT challenges and gain complete network visibility. For more information, or learn more about the inventor of the first bypass TAP, visit GarlandTechnology.com or @GarlandTech.

About Bricata

Bricata is the leader in comprehensive network protection. The Bricata solution provides unparalleled network visibility, full-spectrum threat detection, threat hunting, and post-detection response capabilities in an intuitive, tightly integrated, and self-managing system. Its automated detection, productive GUIs, and expert system workflows make it easy-to-use for novices, while granular control of its engines, access to rich network metadata and PCAPs, and threat hunting capabilities give experts the power and control they demand. Bricata has been proven to speed incident resolution by up to eight times by reliably detecting threats and providing the context necessary to get to the truth quickly and act. For more information visit www.Bricata.com

Learn More
GarlandTechnology.com/Bricata

Let's Talk
+1 716.242.8500
sales@garlandtechnology.com

GARLAND TECHNOLOGY
See every bit, byte, and packet®