Detect. Decrypt. Deter.

JOINT SOLUTION BRIEF

Garland Technology and Mira Security Provide Complete Network Access and Visibility into TLS Traffic

Business Problems

Nearly all network traffic is encrypted today. It has become the trusted standard that most users and applications expect, and has been deployed across almost every organization due to its ease of use. However, this adoption has created challenges for security teams who are tasked with protecting an organization due to an effective "blind spot" into what is actually happening or included in that encrypted traffic. It has now become clear that, in order to protect an organization and ensure legal and regulatory requirements are met, enterprise security teams need at least some level of visibility into encrypted SSL/TLS traffic.

Technical Considerations

Encrypted network traffic is the norm in enterprise networks today, with over 90% of north/south traffic being encrypted, and over 65% of east/west traffic, as well. Currently, only TLS 1.2 and TLS 1.3 are recommended. Earlier versions of TLS are still encountered in legacy devices, which can create additional visibility challenges as TLS 1.3 improves the security provided through encryption, but reduces the visibility for security devices that do not decrypt traffic. Additionally, the security tools that are looking for visibility into the encrypted traffic need to be sure they are seeing 100% of the traffic flow, even during potential DDoS attacks.

Joint Solution Benefits

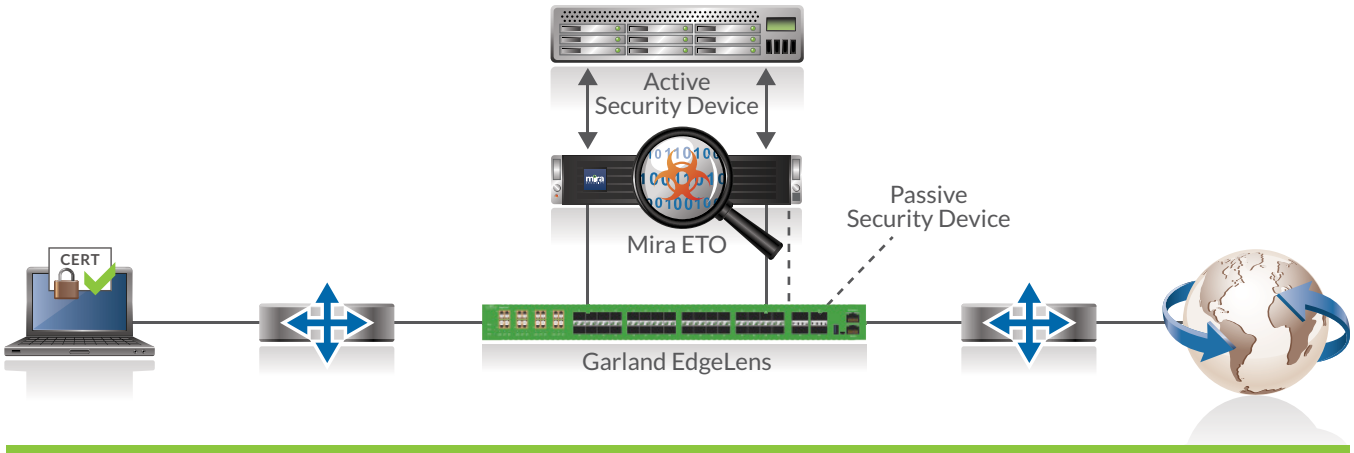
- **Visibility:** The ETO eliminates SSL/TLS blind spots, allowing security tools to detect traffic that might otherwise be hidden by encryption. The ETO is capable of decrypting SSL v3, TLS 1.0, 1.1, 1.2, and 1.3, as well as SSHv2.
- **Connectivity:** The Mira ETO and Garland Inline Bypass appliances are available with 1G, 10G, 25G, and 40G interfaces.
- **Flexibility:** Port-agnostic decryption allows the ETO to decrypt on more than just port 443.
- **Rules and Filtering Options:** The ETO's Category Database can be used to bypass certain categories of traffic and protect sensitive user data, while EdgeLens Filter Templates can be used to choose the type of traffic flows "UDP/TCP" before sending it to its corresponding tool.
- **Ease of Use:** Both the Mira ETO and the Garland EdgeLens are easy to install, configure, and integrate with other elements of your security tech stack.
- **Purpose-Built and High Performance:** Both the Mira ETO and the Garland EdgeLens are purpose-built products allowing for high performance, since the EdgeLens can load balance the decrypted traffic across multiple security and monitoring tools.

Mira Security and Garland Technology Solution

Garland Technology's innovative EdgeLens® is a hybrid bypass TAP and network packet broker solution. It is purpose-built to give you the power of a bypass TAP to manage the availability of inline tools, instrument high availability (HA) deployments, and tool chaining. It also provides packet visibility for out-of-band/passive tools like threat detection, storage, and performance monitoring, as well as providing traffic aggregation, filtering, and load balancing due to its packet broker functionality.

EdgeLens is installed inline at the network edge, managing the risk of downtime due to oversubscribed devices or device failures that can bring down the network, by using heartbeat packets that are configured to monitor the health of inline appliances. They are added by the Bypass TAP component of EdgeLens, and both the live network traffic and the heartbeat packets are sent out to the input port on the inline device, in this case, Mira Encrypted Traffic Orchestrator (ETO). The Mira ETO receives 100% of the network traffic flow from the EdgeLens, allowing it to actively decrypt the network traffic when the SSL/TLS handshake occurs. The ETO can then pass the plaintext data to other inline and/or out-of-band security and monitoring tools for analysis. Then it re-encrypts the data and combines it back with the heartbeat packets, which is sent back through the Bypass TAP, which strips the heartbeat packets before sending the fully re-encrypted traffic back into the live network. Heartbeats are never sent into the live network. If the heartbeat is not received back, indicating that the ETO is offline for some reason, it will automatically bypass the device, keeping the network up even though the device is offline. No network downtime. No single points of failure.

Together, Garland Technology and Mira Security are capable of increasing performance and enhancing the effectiveness of your security and monitoring tools by removing any blind spots in the enterprise network.



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 the USA. 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 or @garland-technology-llc.

MiraSecurity.com

info@mirasecurity.com

Mira Security
3159 Unionville Road, Suite 100
Cranberry Township, PA 16066
Phone: +1 (412) 533-7830

Email: info@mirasecurity.com
mirasecurity.com

MIRA-GARLAND-3/23