Detect. Decrypt. Deter.

JOINT SOLUTION BRIEF

Comprehensive Network Security through Total Visibility into Any Encrypted Traffic

The latest encryption protocol, TLS 1.3, is significantly more complex to decrypt and analyze traffic for security, a task now more critical than ever amid growing threats. Axellio, Garland Technology, and Mira Security have joined forces to provide a centralized, scalable, and affordable solution to decrypt enterprise traffic for full analysis while enhancing access to richer event data for forensic analysis.

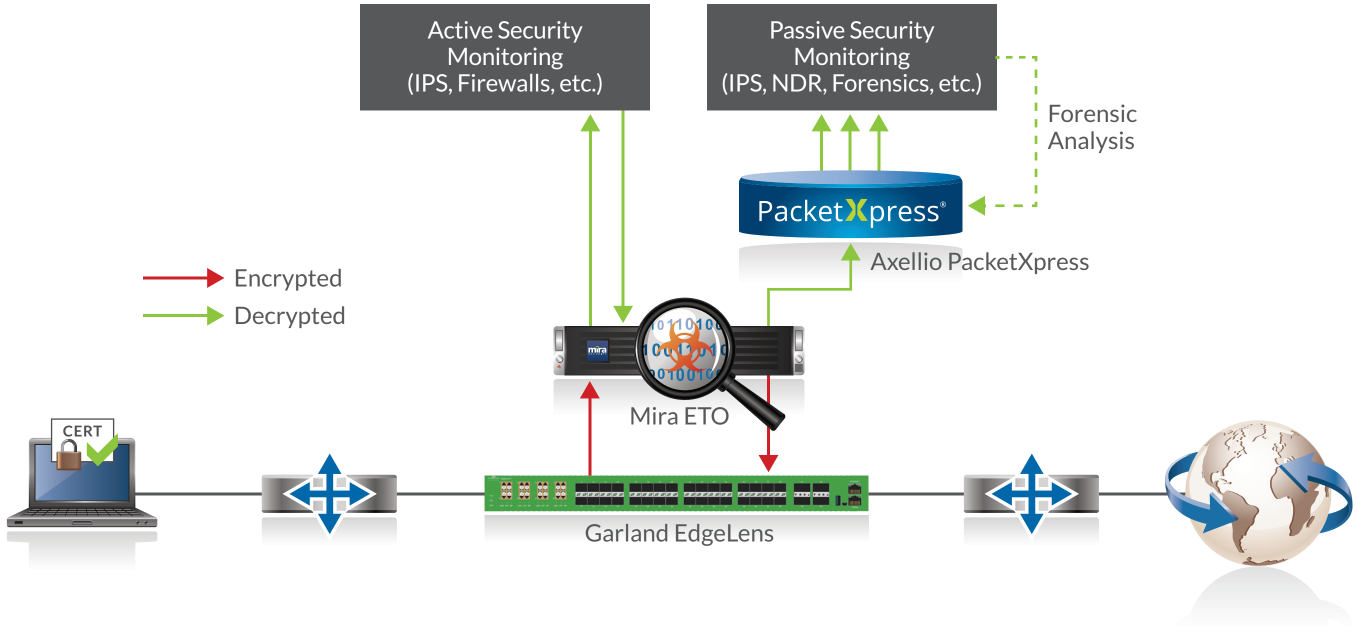
New TLS Version Creates Significant Visibility Challenges, Increasing Security Risks

As businesses demand end-to-end communication privacy and security, network traffic encryption is widely used today, with over 90% of external (north/south) traffic and over 65% of the internal (east/west) traffic being encrypted. Previous versions of the TLS encryption allowed for some analysis. However, the growing adoption of the latest TLS 1.3 version significantly complicates visibility into the encrypted traffic. And, to make matters worse, threat actors are using this to their advantage and encrypting all their communication, making it impossible to analyze. All these factors create significant blind spots for security operations by not being able to analyze this encrypted traffic. However, enterprise security teams need visibility into encrypted TLS traffic at scale across their infrastructure, both external and internal, to protect their organizations and ensure that legal and regulatory requirements are met.

Axellio, Garland, and Mira Security – Visibility into Any Traffic Across the Network

The security and complexity of TLS 1.3 makes it too complex to have each monitoring application decrypt their own traffic, as TLS 1.3 requires the decryption application to be inline and part of the encryption chain. Therefore, Axellio, Garland, and Mira Security have joined forces to provide a centralized, scalable, and affordable solution to decrypt the traffic for all enterprise analysis needs while enhancing access to richer event data for forensic analysis. The combined solution ensures complete network visibility and captures, decrypts, stores, and distributes over 100 Gbps for all existing security analysis systems without overloading them:

- Garland Technology's innovative EdgeLens® is a hybrid bypass TAP and network packet broker solution that is deployed inline at strategic points in the network to capture essential traffic for analysis.
- Mira Encrypted Traffic Orchestrator (ETO) allows decryption of any encrypted traffic reliably and at scale for easy analysis for active and passive security analysis systems.
- Axellio's PacketXpress® provides a high-speed, application-agnostic, open platform that simultaneously captures, stores, and distributes packets. Its unique architecture ensures that existing analysis systems will keep up with any traffic rates for real-time analysis, and provides critical data for forensic analysis.


Active Security Monitoring (IPS, Firewalls, etc.)
Passive Security Monitoring (IPS, NDR, Forensics, etc.)
Forensic Analysis
PacketXpress®
Axellio PacketXpress
Encrypted
Decrypted
mira
Mira ETO
CERT
Garland EdgeLens

Enhance Performance and Effectiveness of Existing Security Monitoring Systems

Together, Garland Technology, Axellio, and Mira Security will increase the performance and enhance the effectiveness of existing enterprise security and monitoring solutions:

- **Eliminate blind spots:** Allow enterprise security tools to detect traffic that might otherwise be hidden by encryption, decrypting SSL v3, TLS 1.0, 1.1, 1.2, and 1.3, as well as SSHv2. The Mira ETO is a port-agnostic appliance that allows decrypting on more than just port 443.
- **Collect anywhere at any speed:** Collect traffic from the physical ingress-egress, the internal network, to virtual and cloud infrastructure. Guarantee no-loss capture at any speed – from a few Gbps to well over 100 Gbps sustained simultaneous data ingest, recording, and distribution.
- **Adaptive traffic distribution and load balancing across multiple analysis applications:** Distribute traffic at controlled, application-consumable rates with no loss. Rewind, replay, and re-analyze for repeated in-depth analysis, mitigation validation, and training.
- **Protect sensitive data:** Mira's ETO rules and filtering options allow you to bypass the decryption of specific categories of traffic and protect sensitive user data.
- **Store for in-depth forensic analysis:** Simultaneous read and write at over 100 Gbps for on-disk storage for days, weeks, or months to ensure you have all the data surrounding any event – even days or weeks later.
- **Ease of Use:** Easy to install, configure, and integrate with other elements of the enterprise security monitoring and analysis infrastructure.

Better Security through Market-Leading Technology

This combined solution provides complete visibility into all encrypted network traffic to fill in the visibility gaps for security devices that do not decrypt their own traffic:

Mira Encrypted Traffic Orchestrator (ETO)

Mira ETO automatically detects SSL, TLS, and SSH traffic and feeds it to one or more security tools that detect and mitigate any threats that may be present. No unnecessary interfaces or software changes are required for the security tools. They receive the decrypted traffic from Mira ETO as if it was traffic directly from the network. This allows for existing security stacks to regain their effectiveness, as these encrypted flows may now be inspected for threats without the need for changes or upgrades to the security stacks.

Axellio PacketXpress®

Axellio® PacketXpress® captures, stores, and distributes all network traffic in an extremely small footprint at over 100 Gbps with no loss. PacketXpress' unique patented capability is to record traffic on disk while simultaneously distributing and providing access to all data directly from disk for real-time or forensic analysis applications. This enhances the performance, efficiency, and accuracy of existing enterprise security analysis applications by avoiding overload situations resulting in lost data and blind spots. For historical forensic analysis and mitigation validation, PacketXpress also replays any pre- and post-event packet data at any speed for in-depth analysis.

Garland EdgeLens®

Garland Technology's innovative EdgeLens® is a hybrid bypass TAP and network packet broker solution. It is purpose-built to provide 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 provide traffic aggregation, filtering, and load balancing due to its packet broker functionality.

About Axellio

Axellio is an innovator in network intelligence platforms for the Department of Defense, the Intelligence Community, and global security operations. With its 20 years of experience in high-speed, high-volume storage, Axellio leverages the latest storage and server architecture technologies for its innovative network intelligence platform, PacketXpress® to capture, store, analyze, and distribute all network traffic in an extremely small footprint at over 100 Gbps with no loss. To learn more, visit Axellio.com.

About Garland Technology

Garland Technology believes network visibility should be an easy, seamless experience. We work with our customers to identify their unique environment requirements and deliver packet visibility to improve their security and monitoring solutions, offering the industry's most reliable, economical, and easy-to-deploy network TAPs, network packet brokers, and inline bypass solutions. To learn more, visit GarlandTechnology.com.

mira SECURITY

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