Gaining Visibility Into Encrypted Enterprise Traffic

Bad actors are now hiding behind TLS 1.2 and 1.3 encrypted traffic. According to a 2022 Zscaler report, 85% of malware is hidden by encryption within network traffic. However, according to the Ponemon Institute's 2021 global encryption trends survey, only about half of organizations are trying to decrypt all of this traffic to stop the malware. Enterprises need to decrypt and inspect this traffic before the attack begins to initiate the components of the cyber kill chain it was programmed for. You need to expose the threat (malware, ransomware, worm, RAT, etc.) before it has a chance to cause significant damage. As several enterprises have found out, the cost of failure can be high. According to the 2024 Keeper Security Insight Report, 73% of respondents that experienced a cyber-attack also experienced a monetary loss in association with that attack. Another report from Halcyon revealed that 57% of respondents said the attacks will have a negative impact long-term on their organization's operations, competitiveness, profitability or even overall viability.

Unfortunately — Many Security Solutions Are Falling Flat

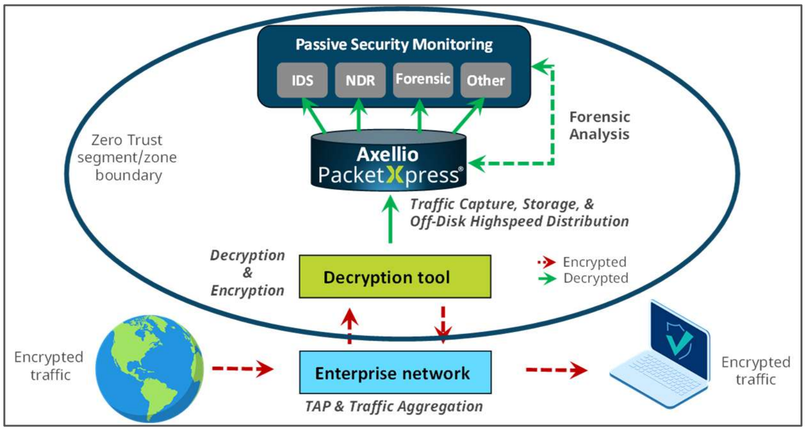
Even though companies are investing in decryption and security tools, many solutions are ineffective. A 2024 Cyware report showed that 49% of respondents ”struggle to derive actionable insights across multiple security tools such as threat intelligence platforms, SIEM, asset management, and vulnerability management platforms.” A 2024 Broadcom report found that 80% of companies are having problems with network visibility and blind spots. Combining these two factoids results in a solution where the security tools could be optimized by adding an out-of-band visibility and data intelligence architecture. The status quo is definitely not working.

Key Components of an Out-of-Band Decryption & Visibility Solution

When looking at an encrypted data visibility solution, there are four key components as follows:

- Decryption tool – Handles data decryption (e.g., TLS 1.2 and 1.3) and re-encryption functions
- Packet data processing functions – High speed data (up to 200 Gbps) processing functionality consisting of data aggregation, filtering, deduplication, high speed data buffering, and distribution to one or more security tools (i.e. threat hunting, DLP, IDS, etc.)
- Data storage – An on-board, high speed, and high-volume secure data storage repository for access by threat hunting and network detection and response (NDR) tools as needed
- Security analysis/threat analysis tools – Provide deep packet inspection (DPI) and threat hunting

The first part of the solution is to use a decryption tool to convert the encrypted data to cleartext data. The second part of the solution is to insert a data intelligence solution, like Axellio’s PacketXpress, that handles data processing and storage to increase visibility. The final part consists of the security tools required for the data analysis. The following figure illustrates how the solution could be implemented.



The Axellio solution handles data processing, data buffering, data storage, and data transmission to the security tool functions. This creates a simple, cost-effective, and completely secure threat detection and analysis solution for enterprise networks.

The Axellio Data Intelligence Solution

Axellio's PacketXpress data intelligence solution delivers the following benefits:

1. Packet data processing features at speeds over 200 Gbps (in a 1U): aggregation, filtering, packet slicing, deduplication, time stamping, and simultaneous data distribution to multiple security tools
2. Data buffering to accommodate bandwidth bursts up to 200+ Gbps
3. High speed data storage (up to 1.2 PB in a COTS 1U server) that allows for fast retrieval of data
4. Secure temporary storage of decrypted data. Decrypt once and then feed multiple tools centralized decrypted data. The Axellio solution allows for faster retrieval without having to redo the decryption process. Data at rest can be encrypted with a single key and stored on-disk for use with in-depth forensic analysis for days, weeks, or months to ensure you have all the data surrounding any event.
5. DVR-like data transmission features that allow play and replay functions which can be used to catch security threats and test security fixes as often as necessary. This feature can be used to locate details about the security threat (e.g. how it moves, what it attacks (edits, deletes, etc.), and to test the efficacy of security fixes to ensure that they stop this specific threat in the future). Rewind, replay, re-analyze features allow for repeated in-depth analysis, mitigation validation, and training.
6. Adaptive traffic distribution and load balancing across multiple analysis applications prevents data loss when connecting to security analysis tools. PacketXpress distributes traffic at controlled, application consumable rates with no data loss.

Contact Axellio and we can show you how to create unparallelled network visibility and optimize your security and monitoring solutions without compromising your network security.

Learn more at: www.axellio.com

Axellio delivers scalable, simultaneous, always-on recording and distribution at over 200 Gbps with no data loss.

For more information, contact us at: www.axellio.com/contact-us/