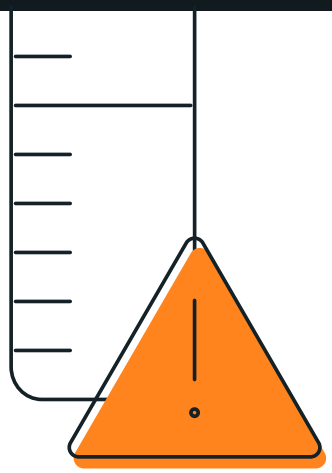
Gigamon® | AXELLIO

Threat Overload – When Traffic Spikes, Gigamon and Axellio Ensure Your Defenses Are On Guard



THE CHALLENGE

When traffic spikes or grows beyond your security monitoring capacity, traffic overload within your security monitoring system and increased levels of encryption make threat detection quickly unreliable.

THE SOLUTION

The Gigamon Visibility and Analytics Fabric™ (VAF) and Axellio PacketXpress work together to ensure that your defenses are not overwhelmed by controlling traffic distribution, avoiding packet loss, while capturing and decrypting packets for in-depth analysis quickly, efficiently — and affordably.

JOINT SOLUTION BENEFITS

+ Gain total visibility into every packet including encrypted traffic –even beyond 100Gbps
+ Access all relevant packet information pre- and post-event – in real-time and for back-in-time analysis
+ Avoid information loss by buffering traffic growth and spikes
+ Reduce time to root cause, cost of downtime and data breaches through visibility into pre- and post-event packet data – PCAP on demand
+ Extend the useful life of your monitoring infrastructure and safely delay costly upgrades by shielding them from intermittent traffic spikes and slow traffic growth

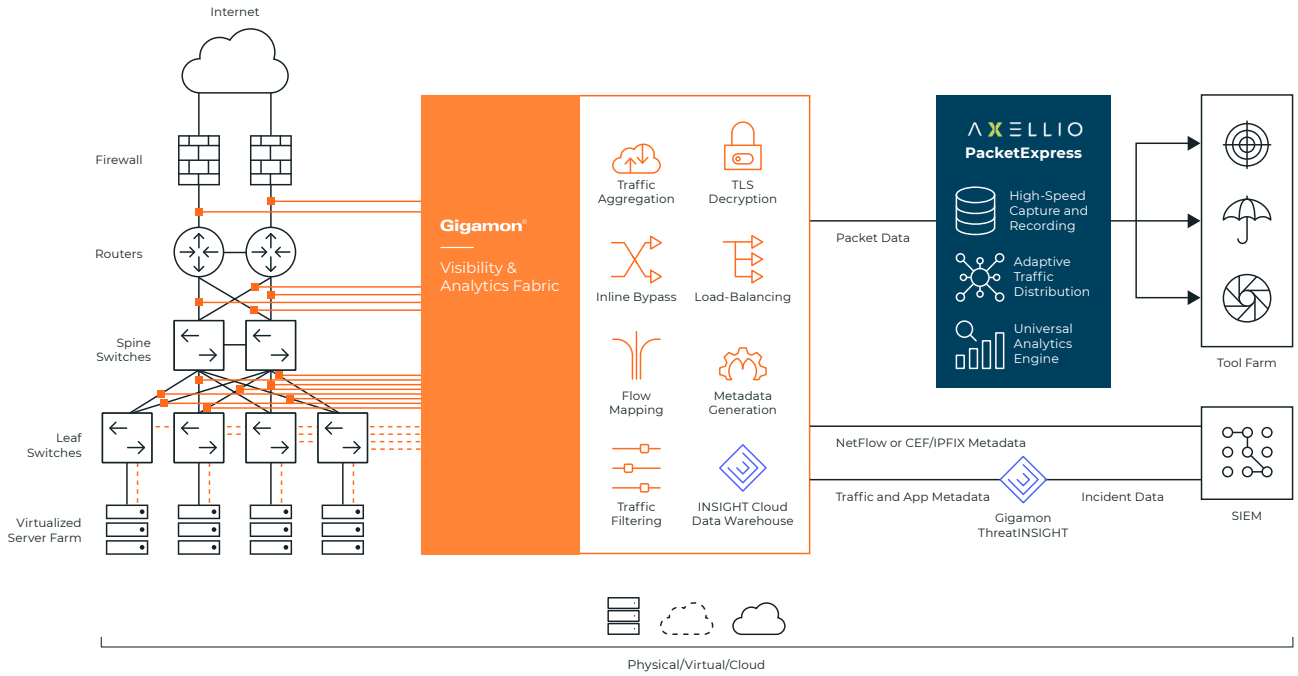
Introduction

By buffering all incoming traffic at sustained rates of 100Gbps with no packet loss, Axellio PacketXpress protects security monitoring and analysis infrastructure from traffic overload. Additionally, because the solution retains captured traffic for weeks or months and provides direct access to all packets of an incident pre- and post-event, it improves threat hunting and analysis. The entire functionality is provided in an economical, small form factor of a single, 3U high rack-mountable appliance.

The Gigamon + Axellio Joint Solution

The combined solution of Gigamon Visibility and Analytics Fabric (VAF) and Axellio PacketXpress adds a new dimension to visibility fabrics – controlling time. In addition to aggregating, decrypting, and managing traffic flows, you are now able to store and forward (i.e. buffer) traffic destined for analysis to avoid overload situations and to go back in time for effective in-depth analysis:

+ **Adaptive traffic distribution to your monitoring & analysis applications:** With the VAF already able to filter out duplicate packets and send only relevant traffic to your monitoring tools, PacketXpress can further adjust the rate to ensure your tools never receive more traffic than they can process.
+ **Easy access to traffic from physical and virtual networks:** The VAF manages and delivers all network traffic — including East-West traffic between applications or workloads within datacenter and private and public cloud environments — to PacketXpress so all traffic can be captured, monitored and analyzed, reducing blind spots and increasing the likelihood of spotting suspicious behavior.
+ **SSL decryption:** With the majority of traffic encrypted, the VAF decrypts SSL encrypted traffic for storage and inspection by PacketXpress and other security tools.



+ **Traffic Aggregation to minimize tools' ports use:** Where links have low traffic volumes, the VAF can aggregate these together before sending them to the PacketXpress to minimize the number of physical ports required. By tagging the traffic, the VAF ensures the source of traffic can be identified.
+ **Easier control of asymmetric routing to help ensure session information is kept together:** Most security devices require that all the packets in a session be inspected by the same device since incomplete sessions risk being blocked – or worse, uninspected! The VAF provides an intelligent and efficient way to help ensure this inspection happens in most architectures.
+ **Masking for security/compliance:** Before storing any information to disk, the VAF masks sensitive or confidential data within packets before they're seen by unauthorized personnel.
+ **Back-in-time analysis for any event:** The VAF decrypts traffic and masks sensitive information before PacketXpress stores the data to disk. This makes it readily consumable for analysis and forensic teams even weeks later for pre- and post-event analysis. With no indexing required, you can extract based on any information needed. There's no need to anticipate what to index before you start the capture or perform lengthy post-capture filtering and analysis procedures.
+ **Hyperscaling:** The VAF can balance the total traffic, in a session-aware manner, across multiple instances of PacketXpress to meet very high traffic loads.

For more information on Gigamon and Axellio, visit: www.gigamon.com and www.axellio.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com