Application Delivery and Troubleshooting with LiveAction and Gigamon Deep Observability Pipeline

Overview

Complex network environments require simple monitoring solutions. Organizations use LiveAction to manage network performance in these environments. Leveraging the Gigamon Deep Observability Pipeline to capture and intelligently route high-fidelity packets or streams of network traffic, LiveAction LiveNX and LiveWire provide intuitive and powerful way to monitor, manage, and troubleshoot applications and network performance for today's enterprise IT environments and provides benefits in the following areas:

Hybrid WAN/SD-WAN Monitoring and Service Assurance

- Cloud Monitoring
- Application Performance and Troubleshooting
- Voice and Video Optimization
- QoS Configuration and Validation
- Root Cause Analysis
- Comprehensive Packet Analytics for Multi-Domain
- Capacity Planning and WAN Bandwidth Management

Joint Solution Benefits

- The LiveAction solution with LiveNX and LiveWire provides a deep understanding of application traffic flows throughout the entire network. The monitoring platform is optimized for collecting flow data at scale and for high-performance packet capture
- Support for real-time visibility and expert analysis of the data center and cloud
- Integration with Gigamon Application Metadata Intelligence (AMI) that extracts close to 6,000 application attributes powered by deep packet inspection to help effectively monitor and manage complex digital applications
- Generating NetFlow/IPFIX from any traffic flow avoids unnecessary processing on network devices and extends visibility to any location or flow within the network
- Masking sensitive data according to industry regulations can help meet compliance

- De-duplicating, aggregating, filtering, and offloading packet processing provides LiveAction an optimized data source in order to ingest packets and accurately represent network flows

The Challenge

Business-critical applications always need to be protected and not impacted by less critical traffic while ensuring security. When there is an application performance problem, 90 percent of the time is spent identifying the root cause as opposed to fixing the problem, and this gets harder with multi-cloud deployments.

The Solution

LiveAction provides end-to-end visibility for network security and performance from a single source of truth. This gives enterprises confidence that the network is securely meeting business objectives, provides full network visibility to better inform NetOps and SecOps as they drive critical decisions for performance and threat response, and reduces the overall cost of network and security operations. By unifying and simplifying the source of collection, inspection, presentation, and analysis of network traffic, LiveAction empowers network and security professionals to proactively and quickly identify, troubleshoot, and resolve issues across increasingly large and complex networks.

The Gigamon Deep Observability Pipeline combined with LiveAction's LiveNX network visualization and analytics platform with LiveWire packet capture and analysis provides the effective visibility and actionable intelligence to optimize your network for business application delivery.

The Gigamon and LiveAction Joint Solution

The Gigamon Deep Observability Pipeline, combined with LiveAction's network intelligence and analytics platform, provides effective visibility and smart analysis to optimize application delivery. This joint solution can provide full packet analytics and visibility into areas of the network where flow data isn't available or is only available as sampled. The solution provides two visibility options:

Flow-Based: Troubleshooting complex problems requires granular flow analysis. LiveAction LiveNX can provide flow visibility across multiple domains in a multi-vendor environment. The Gigamon Deep Observability Pipeline generates NetFlow and application metadata without sampling and provides LiveNX with NetFlow and/or metadata records for real-time and historical analysis. The solution provides scalability, improves data center, cloud, and WAN visibility and accelerates troubleshooting and resolution of performance issues.

Flow and Packet-Based: LiveAction allows for simple workflows from flow data to deep packet analysis. LiveAction LiveWire physical and virtual appliances extend visibility with advanced visual analysis of network, application, and VoIP issues at data centers, public clouds, WAN links, and remote sites and branches. Leveraging intelligent pattern-match filtering in the Gigamon Deep Observability Pipeline to direct only the traffic of interest to one or more LiveWire analyzers provides deep observability to troubleshoot any sized network environment.

How the Joint Solution Works

The Gigamon Deep Observability Pipeline provides LiveAction LiveWire with network traffic as packets and continual NetFlow/metadata records to LiveNX. Network traffic from TAP and SPAN ports are sent to the Gigamon Deep Observability Pipeline. The user specifies which traffic to monitor, and the Gigamon Deep Observability Pipeline passes packets and generates NetFlow/IPFIX records which can be analyzed by LiveAction.

LiveAction leverages packet capture analysis with advanced technologies, such as deep packet inspection (DPI)-based application visibility and SD-WAN and cloud monitoring to provide an effective monitoring solution in the area of application network performance. It uses SNMP to monitor device health, QoS, and other technologies. It leverages APIs from SD-WAN and other fabrics to verify performance and network intent. It can also connect with IT service management (ITSM) solutions like ServiceNow for full operational excellence. It uses flow data (IPFIX and NetFlow) for advanced application and network performance monitoring, conversational data, and the Gigamon Deep Observability Pipeline with Application Metadata Intelligence (AMI).

Employing a variety of data sources, LiveAction visualizes packets and flows across your network topology so you can understand what is happening in your network and the impact on application performance.

Key Gigamon Deep Observability Pipeline features include:

Easy Access to Traffic From Physical Network

The Gigamon Deep Observability Pipeline enables traffic from across the network to be managed and delivered to tools efficiently and in the format they need.

Easy Access to Traffic From Cloud and Virtual Networks

East-West virtualized data center and public traffic is growing increasingly fast. The Gigamon Deep Observability Pipeline is able to acquire this traffic and incorporate it into the deep observability pipeline for delivery to the tools you are using on the virtual or cloud network — ensuring all traffic can be monitored and analyzed together, avoiding blind spots, increasing the likelihood of spotting suspicious behavior, and removing the need to learn a new set of tooling for virtual and public cloud environments.
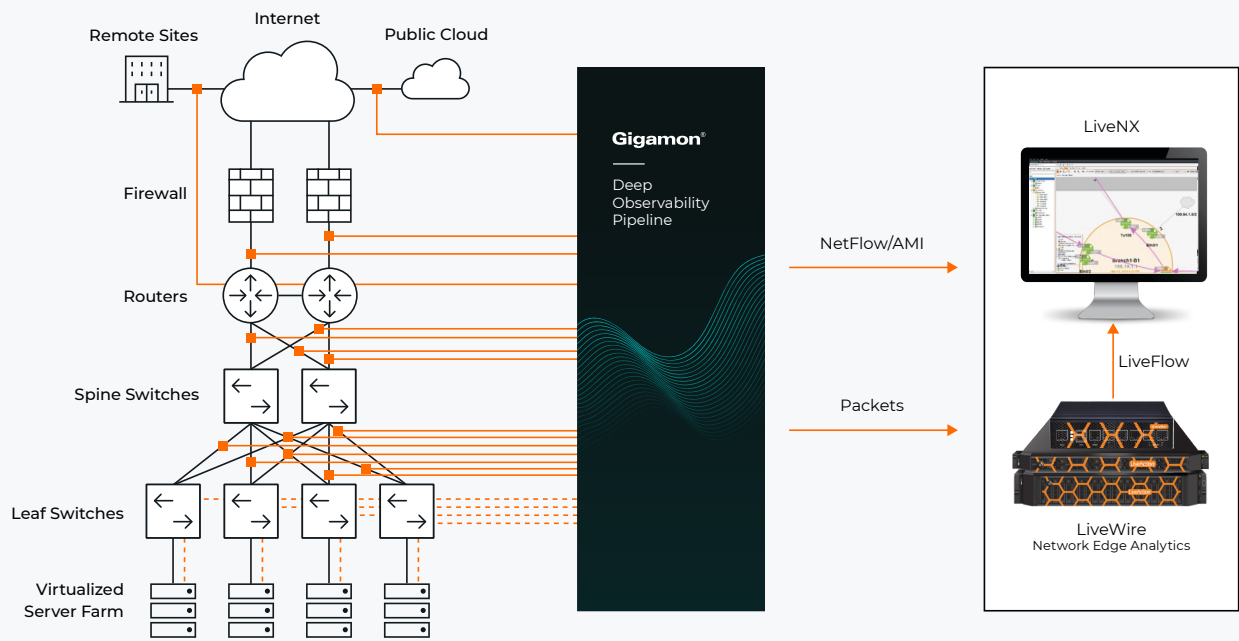

Figure 1. Gigamon and LiveAction Joint Solution Overview (On-premises).

Filtering Traffic to Only Send Relevant Traffic to Tools

There is no point overloading a tool with traffic. The Gigamon Deep Observability Pipeline can be configured to send only relevant traffic to connected tools, based on Layer 4 to 7 criteria and application detection.

Load Balancing to Spread Traffic Across Multiple Devices

When traffic flows are larger than a single tool can cope with, the Gigamon Deep Observability Pipeline can be used to spread the flows across multiple tools while ensuring sessions are kept together and tool numbers can be incrementally grown by adding new devices to those already connected.

Aggregation to Cover Asymmetric Routing and LAG

Where multiple links can carry different packets within the same conversations and multiple feeds may be necessary to capture all packets, the Gigamon Deep Observability Pipeline can aggregate these together before sending the traffic to the tools to ensure each tool sees complete conversations. By tagging the traffic, the Gigamon Deep Observability Pipeline ensures the source of traffic can be identified.

De-Duplication

Pervasive visibility means that you will be tapping or copying traffic from multiple points in the network, which, in turn, means you may well see the same packet more than once. To avoid the unnecessary overhead on your backhaul and tools from processing their packets more than once, the Gigamon Deep Observability Pipeline has a highly effective de-duplication engine to remove these duplicates before they consume resources.
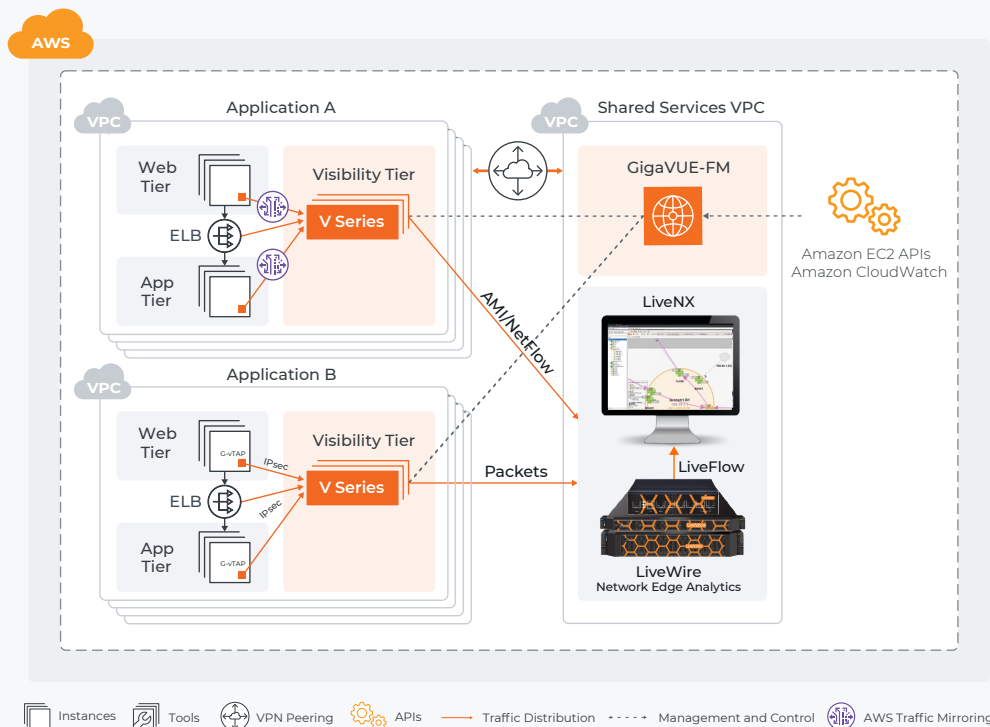

Figure 2. Gigamon and LiveAction Joint Solution Overview (AWS).

Metadata Generation for Deep Application Visibility

Gigamon Application Metadata Intelligence empowers your security information and event management (SIEM) and network performance monitoring tools with close to 6,000 critical metadata attributes across thousands of business, consumer, and IT applications and services. It provides the deep application visibility needed to rapidly pinpoint performance bottlenecks, quality issues, and potential network security risks.

SSL/TLS Decryption

The Gigamon Deep Observability Pipeline can be used to decrypt SSL/TLS-encrypted traffic to allow deeper inspection by security tools and any other devices connected inline or out of band.

Packet or Flow Slicing for Efficiency

If the connected tool doesn't need to see the body information within the packet or most of the packets with flows, the Gigamon Deep Observability Pipeline can selectively remove it before sending the packets to the tool for processing. This reduces load on the device and increases its efficiency.

Masking for Security/Compliance

Certain industries and certain information have to be handled carefully (for example, credit card numbers in e-commerce or patient identification data in healthcare records). The Gigamon Deep Observability Pipeline can be used to mask any sensitive data within packets before they are sent to other tools where they may be seen by operators or others.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

For more information on Gigamon and LiveAction please visit
gigamon.com | liveaction.com

Gigamon®

03.24_09