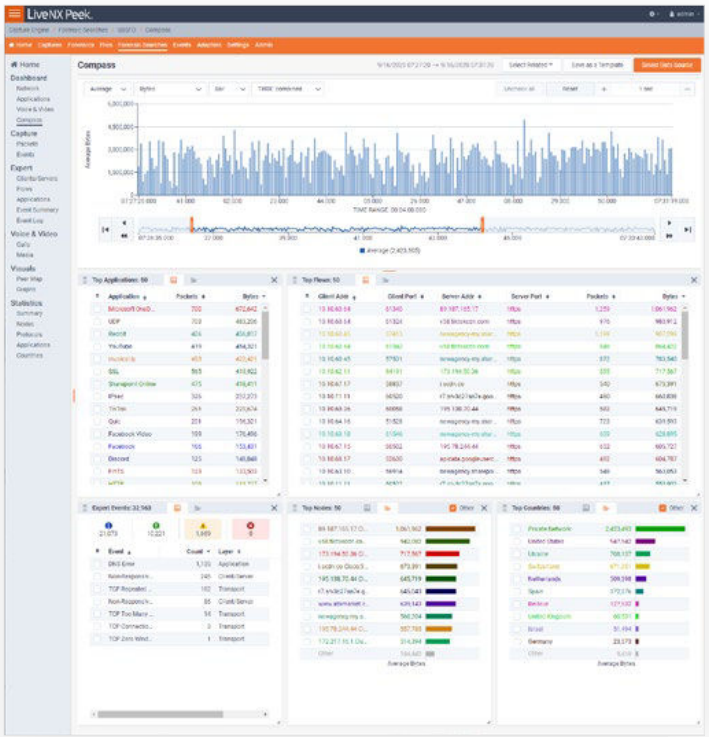
LiveWire
Data Sheet

THE CHALLENGE

There's more data than ever on business networks as these networks expand from the data center to WAN edge to remote sites and cloud. Getting visibility across the entire network and troubleshooting networked applications fast is difficult. Most organizations use a host of network monitoring tools to analyze flow and packet data. Using multiple tools makes solving issues time consuming, impacting mean time to resolution (MTTR).



Packet-level, forensic analysis showing top applications, top flows, detected errors, top nodes, and top countries.

THE SOLUTION

LiveWire high-performance packet capture software integrates seamlessly with LiveNX to extend network monitoring and application troubleshooting to remote sites and branches, WAN edge, and data centers. LiveWire enables real-time and post-event analytics up to 20Gbps and is perfect for capturing packets from virtually anywhere in the network.

LiveWire has deep integrations into LiveNX so you can now easily transition from flow-level to forensic-level analysis and back – in a single software solution. LiveWire uses LiveFlow to convert packet data into rich flow data based on IPFIX, and automatically exports this data into LiveNX. With LiveNX, it's easy to quickly identify and resolve application issues, such as VoIP and video performance problems, without the need for deep forensic analysis.

However, if you need to take a deep dive into packet analysis, you can easily transition from flow to deep packet inspection as LiveWire captures real-time packet data for deep forensic analysis using LiveAction's renowned Omnipeek software.

KEY BENEFITS

Achieve detailed visibility
Make the highest-quality flow data available from anywhere in your network, especially remote offices where flow data are often lacking, to increase visibility and decrease MTTR. Scalable packet to flow data for detailed visibility anywhere, from remote offices to data centers to Cloud.

Accelerate troubleshooting
Detailed troubleshooting requires detailed data, and for network and application troubleshooting the most detailed data available are the network packets themselves. Workflow and automation drive users to the root cause of network and application issues, increasing productivity and reducing the number of solutions (or screens) needed to solve problems.

Optimize security and compliance
Standards compliance and security investigations require the most comprehensive data available, network packets, to effectively report on and investigate issues, whether for routine reporting, detailed investigation, or unequivocal proof.

KEY CAPABILITIES

Digital Transformation
Digital transformation drives increased machine-to-machine, or east-west traffic within data centers, most of which remains invisible to IT teams. These blind spots are prevalent and can be costly.

- Granular insights in a single pane of glass to quickly identify, troubleshoot and resolve issues across the traditional network and into the virtual infrastructure.
- Deep integration with LiveNX lets you easily transition from flow-level to forensic-level, packet-based analysis using a single software solution when flow information just isn't enough.
- Easily and quickly capture packets to automatically identify common issues, from Layer 2 to Layer 7, for network, application, VoIP, and WiFi issues

On-going, End-to-End Monitoring and Troubleshooting

Application performance monitoring is critical in keeping your business working smoothly, yet applications are being virtualized and migrated to the cloud at breakneck speed. This creates blind spots, leaving IT organizations dependent on flow logs and APIs for application performance monitoring.

- Gain a holistic view of network and application events by converting packet data into rich flow-based data using IPFIX and automatically export into LiveNX to quickly identify and resolve issues without the need for packet-level analysis
- Eliminate time wasted reproducing a problem – packets record exactly what happened
- Ability to go directly to packet data to see application errors in packet payloads

Optimized for Highly Distributed Organizations

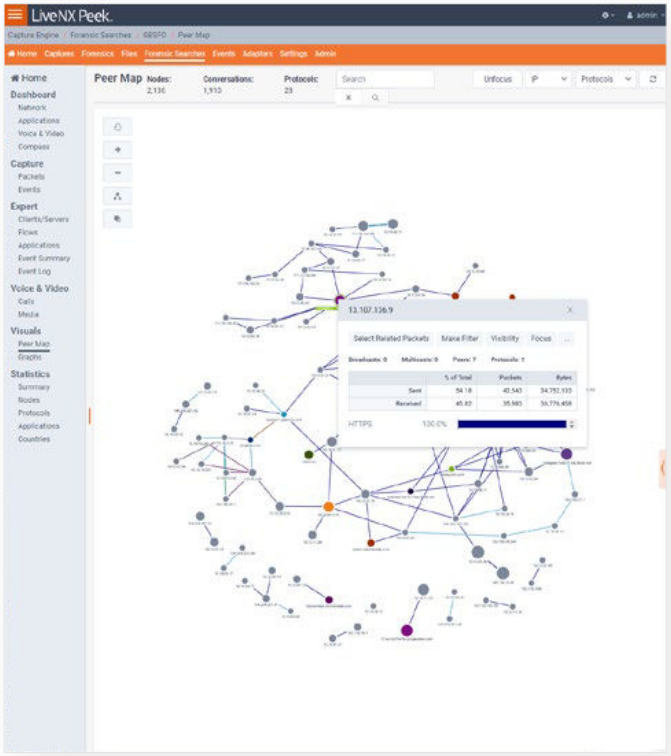
IT organizations struggle to find a cost-effective solution that provides visibility across large numbers of branches and remote locations. What's needed is a solution that can be widely distributed and easily managed, providing true end-to-end visibility.

- Dedicated, scalable software extends flow-based network and application monitoring to remote sites, branches, WAN edge, LAN and data centers
- Scalable packet capture and forensic solutions to handle any network speeds
- Easily identify and quickly resolve network issues with both flow and packet data on a single platform

Security Incident Response

When it comes to security incident response, there's nothing more valuable than the packets themselves. You may have the finest IDS/IPS/SIEM solution available, but once the intrusion is found, what's next? You need a recording of the activity – the network packets – to determine both the fingerprint and extent of the breach.

- Security solutions generate alerts while network packets provide the answers
- Line-rate packet capture with lossless capture-to-disk performance based on scalable hardware and software solutions
- Forensic search terabytes of data without disrupting high-speed storage
- Scalable storage solutions for long-term packet retention ensures regulatory compliance and protects transaction integrity



Detailed flow analysis showing all IP to IP conversations, and highlighting the activity from a node of interest.

Tuned for Your Specific Needs

- **LiveWire has three sizing options:** small, medium, and large to meet your specific needs. The small option is best suited for monitoring remote, lower-bandwidth locations. The medium option works well in small data center settings. And the large option is needed for larger virtual data center operations, or when monitoring high-speed north-south traffic from the virtual server farm.

- **LiveWire can be configured to operate in a number of deployment scenarios** including monitoring/capturing through the standard/distributed virtual switch (vSwitch), monitoring/capturing through the tunneled overlay network, and monitoring/capturing through a virtual tap (vTap) or virtual packet broker (vPB). LiveWire can also be purchased as a hardware appliance.

Learn More

For more information about LiveWire specifications, please visit: liveaction.com/livewire

About LiveAction

LiveAction provides end-to-end visibility of network and application performance from a single pane of glass. This gives enterprises confidence that the network is meeting business objectives, offers IT administrators full visibility for better decision making, and reduces overall cost of operations. By unifying and simplifying the collection, correlation and presentation of application and network data, LiveAction empowers network professionals to identify, troubleshoot and resolve issues across increasingly large and complex networks proactively and quickly.