LiveAction
A BlueCat Company

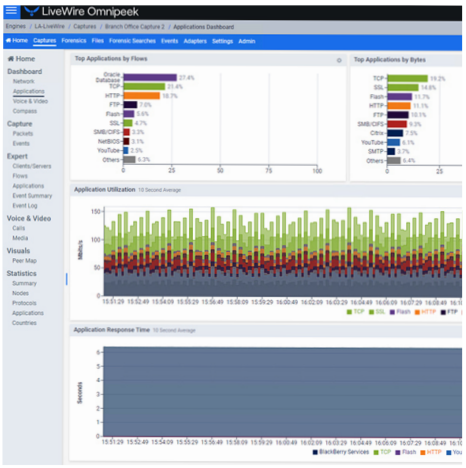
Capture and analyze packet data

Extend monitoring and troubleshooting to your most important network segments with scablable, real-time packet analysis

Network visibility challenges in modern distributed environments

As networks expand from the data center to the WAN edge, remote sites, and cloud, it is increasingly difficult to have visibility across the entire network and quickly troubleshoot networked applications. Most enterprises use a host of network monitoring tools to analyze operational data. But using multiple tools makes solving issues time consuming, impacting mean time to resolution (MTTR).

The solution: LiveWire



BlueCat LiveWire is a high-performance packet analysis solution that captures and stores detailed packet data for network and application performance and forensic insights. By deploying LiveWire physical or virtual appliances in your most critical network segments—including data centers, SD-WAN edges, the cloud, and remote sites—your network and security operations teams have the data they need to ensure the performance and security of your network.

LiveWire captures real-time packet data. When you need to examine packets for deep forensic analysis, LiveWire offers an easy-to-use interface, advanced visualizations, built-in workflows, a built-in expert system, and many different types of analysis and correlations. LiveWire is built to accelerate troubleshooting and deliver the packet data and packet analysis you need for advanced network forensics.

In addition, LiveWire delivers enriched packet data to BlueCat's LiveNX network performance management platform. This makes it easy to transition from flow-level to forensic-level analysis and back—all on a single platform. LiveWire converts packet data into rich flow data and automatically exports the data into LiveNX. With LiveNX and LiveWire, it's easy to quickly identify and resolve application issues, such as VoIP and video performance problems, without the need for deep forensic analysis.

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. Instead, LiveWire delivers:

- Granular insights to quickly identify, troubleshoot, and resolve issues across your traditional network and into virtual infrastructure.
- Easy and quick packet capture to automatically identify common issues, from Layer 2 to Layer 7, for networks, applications, VoIP, and Wi-Fi.
- Intelligent packet capture, which saves precious disk space by detecting encrypted traffic and automatically slicing off payloads when this feature is turned on.
- LiveFlow web analytics for enhanced flow data with specific web application metrics—such as URL or URI, page response times, and error response codes—even when traffic is encrypted. This provides key performance indicators for monitoring custom web applications.

- When flow information just isn't enough, deep integration with LiveNX to transition from flow- to forensic-level packet-based analysis using a single software solution.

Ongoing, end-to-end monitoring

Application performance monitoring is critical for keeping your enterprise running 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. LiveWire helps you:

- Gain a holistic view of network and application events by converting packet data into rich flow-based data using telemetry. The data is automatically exported 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.
- Go directly to packet data to see application and network errors in packet payloads.

Enterprise-grade management

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

- Enterprise-scale management of thousands of LiveWire devices with LiveWire Grid, a web-based management and configuration console.
- Dedicated, scalable software that extends flow-based network and application monitoring to data centers, the WAN edge, remote sites, branches, and the LAN.
- Scalable packet capture and forensic solutions on a single platform that can handle any network speed to easily identify and quickly resolve network issues with both flow and packet data.
- Packet storage that scales to your needs—LiveWire offers field-upgradable storage for its PowerCore appliances of up to 2+ PB of raw storage and 6+ PB of effective storage using compression and/or slicing.

LiveWire Grid

LiveWire Grid is a software as a service (SaaS) solution that simplifies and scales the management and administration of LiveWire devices, no matter how many are deployed. With LiveWire Grid, you get:

- Efficient management of thousands of LiveWire devices—physical, virtual, or cloud
- Streamlined installation and ongoing administration for an exceptionally low total cost of ownership
- Configuration management from a single SaaS console
- Template-based mass configuration push
- Cloud-based backup and restore for easy, efficient roll-backs
- Single sign-on
- An improved user experience while reducing operational overhead
- Reduced hardware costs and lower maintenance costs

Security incident response

When it comes to security incident response, there's nothing more valuable than the packets themselves. You may have the finest intrusion prevention and detection and/or security event management 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. With LiveWire, you get:

- Network packets that provide answers; meanwhile, security solutions only generate alerts.
- Line-rate packet capture with lossless capture-to-disk performance based on scalable hardware and software solutions.
- The ability to perform forensic searches on terabytes of data without disrupting high-speed storage.
- Scalable storage solutions for long-term packet retention, which ensures regulatory compliance and protects transaction integrity.

Features

Network-wide visibility
Make the highest quality flow data available from anywhere on your network—especially your most critical segments—to increase visibility and decrease MTTR. Scalable packet flow data delivers detailed visibility from anywhere across the network, including data centers, the WAN edge, cloud, and remote sites.

Accelerate troubleshooting
Detailed troubleshooting requires detailed data. For network and application troubleshooting, the most detailed data available is the network packets themselves. Workflows and automation drive users to the root cause of network and application issues. The result is increased productivity and a reduced number of solutions (or screens) needed to solve problems.

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

Tuned for your specific needs

LiveWire includes physical, virtual, and cloud offerings, and can be deployed based on your network's specific needs. LiveWire physical appliances offer massive scalability and performance to support network operations for the largest networks, from branch offices to large data centers to the WAN edge. LiveWire virtual and cloud offerings scale with your needs and deliver the flexibility required in these networking environments.

For organizations with many branch locations, such as banking and retail, LiveAction offers the LiveWire Edge. The LiveWire Edge is a small form factor appliance with no moving parts that is simple to install and manage. It is perfect for organizations with an IT department that is already stretched thin.

LiveWire device	Edge	Core	PowerCore	StorageCore	Virtual
Use cases	Remote offices, retail outlets, warehouses, bank branches, and more	Large branch or WAN edge	Data center	Data center	Monitoring virtual and cloud environments
Network ports	4×1G and 1x pass-through	4×1G 2×10G 4×10G	4×10G 4×25G 2×40G 2×100G	4×10G 2×40G 2×100G	Configurable
Raw storage	1 TB SSD	32 TB	240 TB	1.44 PB	Configurable
Effective storage	N/A	96 TB	720 TB	4.32 PB	Configurable
Storage expansion - RAW	N/A	N/A	1 PB+; 240 TB increments	N/A	Configurable
Dimensions and weight	8.5×5.7×1.7 in 2.6 lbs	1 U 48 lbs	2 U 80 lbs	4 RU 200 lbs	N/A

LiveWire on Cisco UCS device	C220 M5 Rack Server	C240 M5 Rack Server	S3260 Storage Server	Virtual
Use cases	Large branch or WAN edge	Data center or service point edge	Data center	Monitoring virtual and cloud environments
Network ports	4×1G 4×10G 2×40G	4×10G 2×40G 2×100G	4×10G	Configurable
Raw storage	24 TB	240 TB	1 PB	Configurable
Effective storage	72 TB	720 TB	3 PB	Configurable
Dimensions	1 U	2 U	4 U	N/A

BlueCa's Intelligent Network Operations (NetOps) provide the analytics and intelligence needed to enable, optimize, and secure the network to achieve business goals. With an Inteligent NetOps suite, organizations can more easily change and modernize the nework as business requirements demand.

Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
Phone: 1-416-646-8400 I 1-866-895-6931

bluecat.com

Next steps

Discover how LiveWire's packet analysis can help ensure the performance and security of your network.

Get in touch