

Capture and analyze packet data

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

Network visibility challenges in modern distributed environments

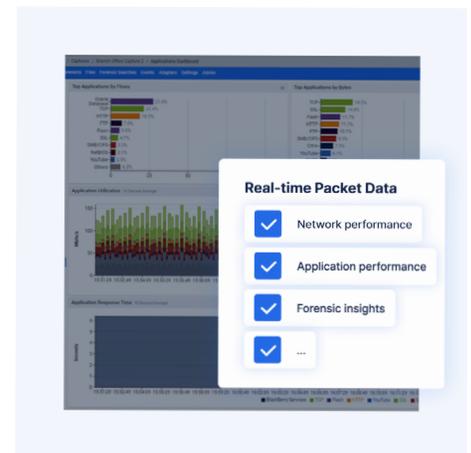
As networks expand from the data center to the WAN edge, remote sites, and cloud, it is increasingly difficult to have visibility across the entire network and quickly troubleshoot networked applications. Most enterprises use a host of network monitoring tools to analyze operational data. But using multiple tools makes issue resolution time-consuming, increasing 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 network performance and security.

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, an expert system, and many types of analysis and correlation. 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 solution. 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 it to 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**
Rising machine-to-machine (east-west) traffic in data centers creates costly blind spots. LiveWire delivers:
 - Granular insights to quickly detect and resolve issues across physical and virtual networks.
 - Fast packet capture to identify issues from Layer 2 to 7 for apps, VoIP, and Wi-Fi.
 - Intelligent capture that saves disk space by detecting encrypted traffic and slicing payloads.
 - LiveFlow web analytics with key metrics (URL/URI, response times, error codes) for visibility—even in encrypted traffic.
- ✓ **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 to LiveNX, enabling quick identification and resolution of issues without 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:

- Centralized management of LiveWire devices via LiveWire Grid's web console.
- Scalable software extending monitoring from data centers to branches and WAN edges.
- Unified flow and packet capture at any network speed for fast issue resolution.
- Expandable packet storage—PowerCore supports 2+ PB raw and 6+ PB effective capacity.

✓ **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 reveal both the fingerprint and extent of breaches.
- Lossless, line-rate capture with scalable hardware and software.
- Forensic searches on terabytes of data without disrupting storage.
- Long-term, scalable retention to meet compliance and protect integrity.

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:

- Centralized management for physical, virtual, or cloud devices.
- Simple installation and low total cost of ownership.
- Single console for configuration and mass updates.
- Cloud-based backup and restore.
- Single sign-on and improved user experience.

Features



Network-wide visibility

Make the highest-quality flow data available from anywhere on your network—especially in 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 fewer 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 banks and retailers, LiveAction offers the LiveWire Edge. The LiveWire Edge is a small-form-factor appliance with no moving parts, making it simple to install and manage. It is perfect for organizations with an already-stretched IT department.

LiveWire device	Edge	Core	PowerCore**	Virtual
Use cases	Small or remote office	Large branch or WAN edge	Data center	All
Network ports	4×1G and 1x pass-through	4×1G 2×10G 4×10G	4×10G 4×25G 2×40G 2×100G	Configurable
Memory	32 GB	128 TB	256 TB	Min. 8 GB
Raw storage	1 TB SSD	24 TB	240 TB	Configurable
Effective storage*	N/A	72 TB	720 TB	N/A
LiveFlow export	Up to 1 Gbps	Up to 15 Gbps	Up to 75 Gbps	Up to 4 Gbps
Forensic capture (capture-to-disk)	Up to 1 Gbps	Up to 40 Gbps	Up to 96 Gbps	Depends on hardware
Dimensions and weight	8.5×5.7×1.7 in 2.64 lbs	1U 39 lbs	2U 73 lbs	N/A
Omnipeek for Windows	Yes (1 license)	Yes (1 license)	Yes (1 license)	No

* Assumes a 3:1 data reduction ratio through compression and/or data slicing

** Supports 10 Gbps, 40 Gbps, and 100 Gbps

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

Headquarters

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

bluecat.com

Next steps

Discover how you can capture and store detailed packet data for network and application performance insights.

[Learn more](#)

