LiveAction
A BlueCat Company

LiveWire | Solution brief

Remote Packet Capture Engine

Forensic-grade endpoint visibility to eliminate blind spots and accelerate troubleshooting

Challenge

Enterprises often lack visibility into user endpoints, creating blind spots that hinder troubleshooting and increase risk. Without insight into remote devices, teams struggle to diagnose issues, determine root causes, or analyze traffic outside the corporate perimeter.

Solution

Remote Packet Capture Engine provides forensic-grade endpoint visibility within BlueCat LiveWire, eliminating blind spots, accelerating troubleshooting, and enhancing the remote user experience—all within a single unified observability platform.

Benefits

- Accelerate root cause analysis
- Support remote users
- Detect endpoint threats
- Extend LiveWire's value with seamless, unified visibility into remote device traffic

Contact us

Enabling forensic-grade packet collection and analysis directly from laptops and workstations

Today's enterprise network is no longer confined to the data center. It spans hybrid clouds, software-as-a-service (SaaS) environments, remote offices, and—most critically—endpoints such as laptops and mobile devices used by employees working anywhere.

Many organizations still focus their monitoring and packet capture on core infrastructure and network edges, leaving a major blind spot at user endpoints. Without visibility into what is happening directly on devices, IT and security teams face critical obstacles, including:

- **Incomplete diagnosis:** IT teams cannot isolate application slowness that only occurs on a user's machine without packet data from that endpoint.
- **Extended downtime:** Troubleshooting delays compound user frustration and impact productivity.
- **Uncertain root cause analysis:** Is an issue caused by the corporate wide-area network, SaaS provider, internet service provider, or the device itself? Without definitive packet-level evidence, teams guess rather than know for sure.
- **Security exposure:** Endpoints are common entry points for cyberattacks. If packet data is unavailable, threat activity may remain invisible until it causes real damage.

According to a 2024 IDC report, over 70% of incidents traced back to remote workers begin at the endpoint level. Lacking forensic-grade visibility not only increases risk but also undermines trust between IT teams and business stakeholders.

This solution brief presents how Remote Packet Capture Engine extends the power of BlueCat LiveWire to user endpoints, enabling forensic-grade packet collection and analysis directly from laptops and workstations. This brief offers specific use case examples that provide clarity, accelerate resolution, and maintain smooth business operations. It also highlights key differentiators from other solutions and outlines primary benefits.

Solution overview

As a part of BlueCat's network observability and intelligence offerings, Remote Packet Capture Engine, an add-on to LiveWire, provides teams with clarity to eliminate blind spots, enhance remote troubleshooting, and improve the end-user experience.

Remote packet capture provides definitive data from the source, whether it's a remote employee experiencing application slowness or an executive reporting intermittent connectivity issues.

Instead of waiting for physical access or shipping devices back to IT, network and security teams can:

- Remotely capture live packet data from the user's device—anywhere, anytime.
- Perform forensic-grade analysis on session flows, latency, jitter, and retransmissions.
- Correlate endpoint traffic with infrastructure-level data already captured by LiveWire.
- Eliminate blind spots and create a continuous view from user devices to cloud applications.

This capability transforms the IT team's operating model. What once required hours or days of back-and-forth with frustrated users can now be resolved in minutes with definitive, packet-level evidence.

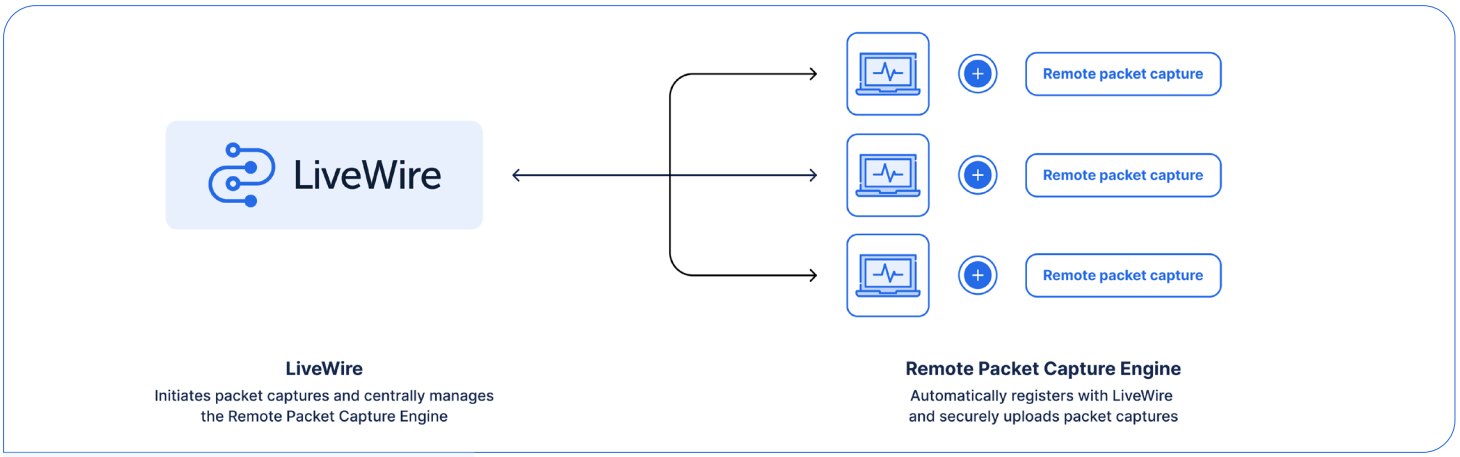

Figure 1: Remote Capture Packet Engine architecture

Five types of use cases

Every second counts when resolving issues that impact users. These use cases demonstrate how Remote Packet Capture Engine delivers instant clarity, empowering network teams to cut through the noise, accelerate resolution, and keep business operations running smoothly.

1. Troubleshooting end-user performance issues

An employee reports intermittent slowness or connection drops in an internal or SaaS application. Remote packet capture allows network operations teams to capture and analyze traffic directly from the user's device, helping them determine whether the root cause is the network, the application, or the local machine.

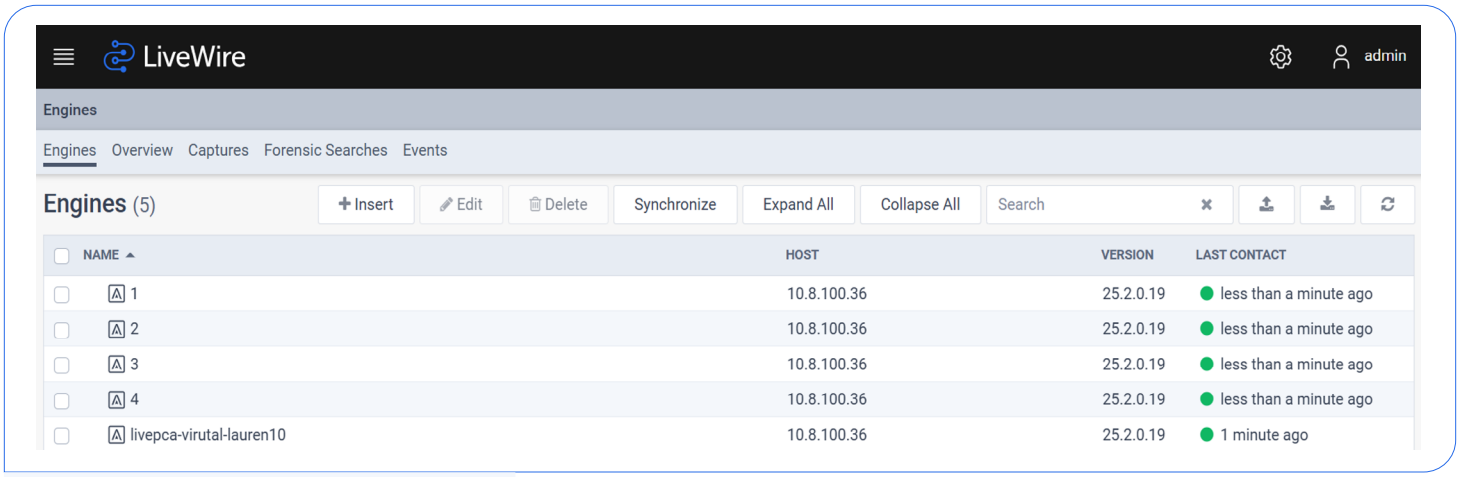

Figure 2: LiveWire dashboard with a list of remote engines

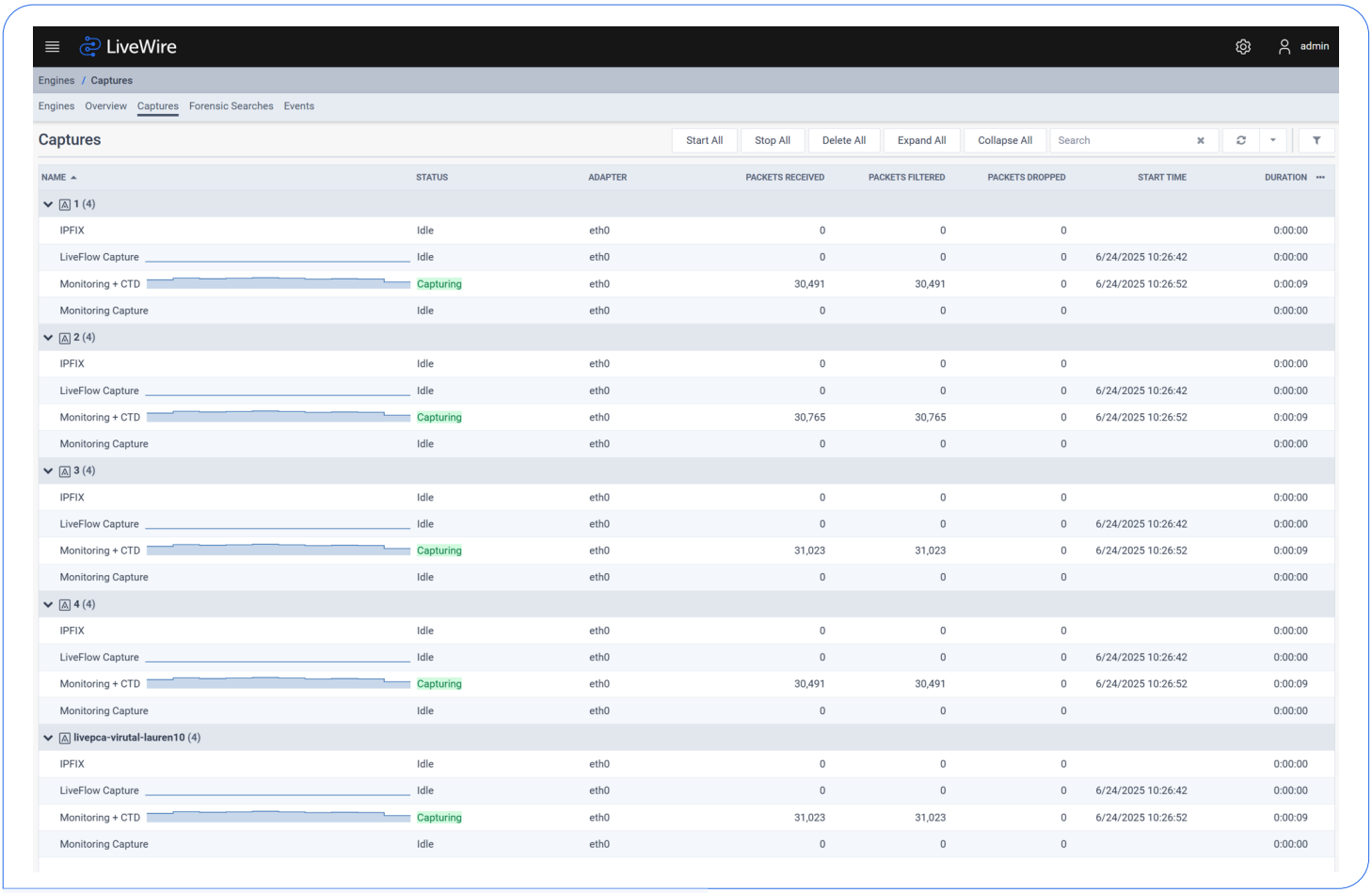

Figure 3: LiveWire dashboard with a list of capture sessions running on remote engines

2. Supporting remote and hybrid workers

IT teams need to diagnose problems for employees working from home, on the road, or outside the virtual private network. Remote packet capture enables end-to-end visibility without requiring physical access to the endpoint, significantly reducing mean time to resolution.

3. Navigating threats at the endpoint

A device shows signs of unusual traffic or a potential breach. Packet-level data from the endpoint helps security teams investigate threats, trace lateral movement, and identify command-and-control traffic.

4. Application-level performance analysis

Users can experience slow performance with specific apps, such as VoIP, video conferencing, or internal business systems. Packet capture at the source provides visibility into session flows, jitter, retransmissions, and latency, helping to differentiate between application, network, and device issues.

5. Executive or VIP user support

A C-level executive reports sporadic connectivity issues or degraded performance. High-priority support teams can initiate a remote capture without disruption, providing immediate and accurate diagnostics.

Key differentiators

Remote Packet Capture Engine is not just another endpoint monitoring tool. It stands apart due to its unique combination of:

1. **Targeted or always-on capture:** Flexible options to maintain continuous collection or initiate packet capture as needed.
2. **Scalable agent management:** Manage thousands of endpoints from the LiveWire interface.
3. **Forensic-grade analysis:** Leverage advanced analytics to dissect traffic down to the packet level.
4. **Secure and lightweight:** Minimize performance impact on endpoints while ensuring secure data transmission.

This combination of scalability, precision, and security extends enterprise-class observability to endpoints without incurring operational overhead.

Solution benefits

Remote Packet Capture Engine offers network operations teams several benefits for remote issue detection and forensic analysis. With Remote Packet Capture Engine, network teams can:

- Accelerate root cause analysis. Quickly determine if issues are network-related or endpoint-specific, without needing physical access to devices.
- Improve support for remote users. Capture and analyze traffic from remote laptops, regardless of location.
- Enhance your security posture. Get insights into endpoint traffic patterns to detect anomalies or malicious activity.
- Maximize return on existing investments. Extend LiveWire's capabilities with endpoint visibility and utilize a unified workflow.

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 I 1-866-895-6931

bluecat.com

Next steps

Learn more about how you can get endpoint visibility to eliminate blind spots and accelerate troubleshooting.

Contact us

SB-LiveWire RPCE-10302025