Riverbed NPM+ Packet Capture Module

Delivering Full-Fidelity Visibility Across Modern Networks

The Visibility Crisis in Modern Networks

Traditional packet capture tools excel at analyzing network traffic moving through data centers and core infrastructure. Riverbed AppResponse, for example, delivers powerful, scalable packet-based analysis across enterprise networks. However, as encryption and Zero Trust architectures have become standard, much of today's critical traffic never traverses those monitored links. Traffic is now commonly encrypted at the endpoint and carried through VPN or Zero Trust tunnels, leaving traditional packet capture tools blind to what happens inside.

As organizations expand across remote, cloud, and hybrid environments, NetOps and SecOps teams lose access to the full-fidelity data they rely on for troubleshooting, threat investigation, and performance optimization. The result is a growing visibility gap, where encryption and secure access controls obscure the details required for even basic root-cause analysis.

Evolving Visibility Requirements for Today's Networks

Encryption, Zero Trust architectures, and distributed application delivery means that traffic patterns are no longer centralized or predictable. Gaining meaningful insight now requires visibility that extends beyond the data center by capturing network behavior where it originates and correlating it across users, devices, and applications.

- **Remote Work:** Expanding the enterprise edge to thousands of users, devices, and locations creates new blind spots in user experience and endpoint performance.

- **Cloud and SaaS:** Decentralized applications and hybrid workloads require visibility across multiple providers, regions, and architectures.

- **Zero Trust:** Continuous verification and encrypted traffic protect data but also limit traditional monitoring approaches.

Modern observability strategies must combine high-fidelity telemetry with intelligent context, enabling IT teams to understand performance and security in real time across hybrid and cloud environments. The next generation of visibility isn't about more data – it's about seeing the right data, wherever it lives.

Bringing Packet-Level Precision to NPM+

Riverbed NPM+ was built for distributed networks where traditional monitoring can't reliably pinpoint root cause. Powered by the Riverbed Unified Agent, NPM+ links performance signals across users, devices, applications, and network paths, so teams can quickly move from symptom to root cause.

As a module included with NPM+, the Packet Capture Module adds full-fidelity packet capture at the endpoint. It captures packets before they traverse VPN tunnels or are encrypted by ZTNA gateways, giving teams definitive packet evidence when metrics alone aren't enough. Combined with NPM+ telemetry, the Packet Capture Module supports deep troubleshooting, forensics, and compliance workflows using standard PCAP file format.

Full-Fidelity Visibility When It Matters Most

Several Riverbed solutions work together to provide complete visibility and analytics.

The NPM+ Core Module provides the first layer of analysis, interpreting packet metadata in motion to surface latency, loss, retransmissions, and delay across applications, servers, and endpoints. For most operational needs, the Core Module delivers the speed and intelligence required for rapid triage and root-cause resolution.

When troubleshooting demands deeper forensics, the NPM+ Packet Capture Module captures and preserves packets on demand, continuously, or on a schedule from any endpoint managed by the Riverbed Unified Agent. Stored locally and harvested securely when needed to customer-designated storage, the Packet Capture Module provides packet-level visibility across Zero Trust, cloud, and remote environments, ensuring critical data is available even when traffic is encrypted or tunneled.

The NPM+ Unified Communications Module extends visibility into collaboration solutions, including Microsoft Teams, Zoom, Webex and Contact Center as a Service (CCaaS) platforms, such as Genesys Cloud. It correlates key UC performance metrics – such as jitter, latency, call quality, and session setup time – with telemetry from the NPM+ Core Module. This unified view enables IT teams to quickly pinpoint whether UC issues stem from the application, network, or device, ensuring consistent voice, video, and customer engagement experiences.

Riverbed IQ Ops completes the picture with dynamic baselining, anomaly detection, correction, and automation. Through IQ Ops workflows, packet captures can be triggered or scheduled based on conditions or alerts, ensuring the right data is collected at the right time. Together with Riverbed IQ Ops, the NPM+ Core, Unified Communications, and Packet Capture Modules support a seamless troubleshooting workflow – from automated performance triage to defensible, packet-level evidence – empowering NetOps and SecOps teams to act quickly and with confidence.
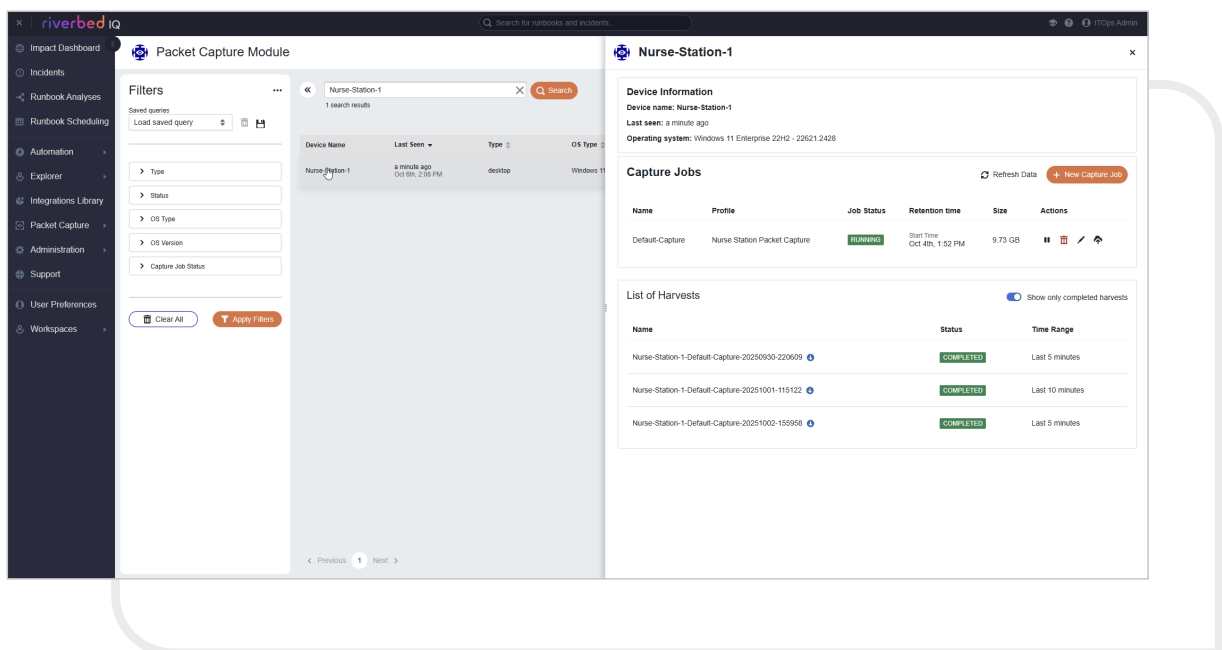
Inside the Packet Capture Module

As enterprises expand into hybrid, multi-cloud, and Zero Trust environments, packet capture must evolve to match modern traffic patterns. The Packet Capture Module is built for this new reality, delivering scalable, secure, and intelligent packet capture wherever traffic originates. It combines endpoint flexibility with centralized control to accelerate investigations, strengthen security, and preserve the packet data that underpins compliance and forensic workflows.

- **Endpoint-Based Capture:** Initiate packet capture through the NPM+ user interface, API, and Riverbed IQ Ops automation. IT Teams can trigger captures instantly or schedule them in advance, collecting the exact data needed without manual intervention or guesswork.

- **Unified Agent Deployment:** Leveraging the Riverbed Unified Agent, the Packet Capture Module deploys seamlessly across diverse endpoints, minimizing administrative effort and eliminating agent sprawl while maintaining consistent, high-fidelity capture quality.

- **Scalable Architecture:** Scales easily across remote, on-premise, virtual, and cloud environments, allowing observability to grow in step with changing infrastructure and user demands without adding operational complexity.

- **Security and Compliance Ready:** Provides verifiable packet evidence to support forensic analysis, audit documentation, and regulatory retention policies. Captured packets remain protected, traceable, and tamper-resistant from collection through retrieval.

- **PCAP File Generation and Access:** Produces standard PCAP files for captured traffic, enabling direct analysis with Riverbed Transaction Analyzer, Riverbed Packet Analyzer Plus, Wireshark, or third-party analysis tools. This preserves familiar investigative workflows while extending your reach into encrypted and Zero Trust environments.

Together, these capabilities make the Packet Capture Module an essential complement to the NPM+ Core and UC Modules, bringing precision packet visibility to every corner of the enterprise and giving NetOps and SecOps teams the confidence that no packet – and no problem – goes unseen.

Figure 1: Packet Capture Module UI gives you complete control over the entire fleet of deployed Packet Capture module agents.
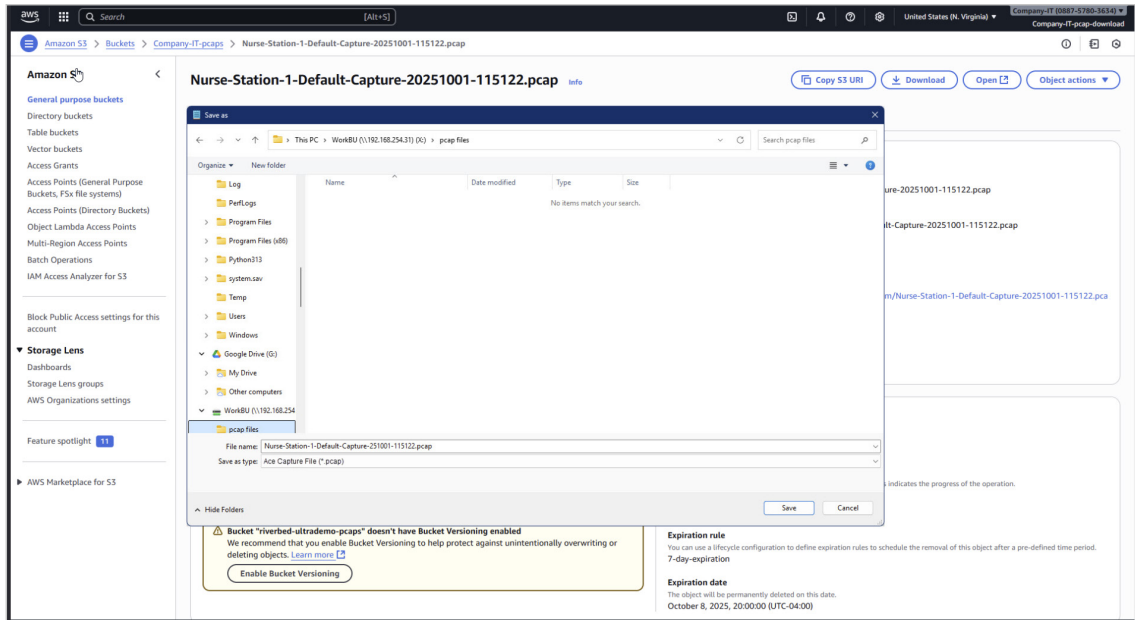
Figure 2: You chose which customer managed storage to use for secure transfer and storage of PCAP files.

Unified Observability Without Compromise

Riverbed NPM+ and the Packet Capture Module bring precision, scale, and intelligence to modern observability. Together with the Core, Unified Communications, and Riverbed IQ Ops, they provide a seamless, intelligent view of network performance and security – from endpoint to cloud, from encrypted traffic to user experience. The result is faster resolution, stronger compliance, and complete confidence in every digital interaction.

Get Started Now

Discover how Riverbed's NPM+ Packet Capture Module can help your organization gain pre-encryption visibility and streamline observability across the enterprise. Visit riverbed.com to learn more or request a demo.

riverbed

About Riverbed

Riverbed, the leader in AIOps for observability, helps organizations optimize their user's experiences by leveraging AI automation for the prevention, identification, and resolution of IT issues. With over 20 years of experience in data collection and AI and machine learning, Riverbed's open and AI-powered observability platform and solutions optimize digital experiences and greatly improves IT efficiency. Riverbed also offers industry-leading Acceleration solutions that provide fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of market-leading customers globally – including 95% of the FORTUNE 100 – we are empowering next-generation digital experiences. Learn more at riverbed.com.