riverbed

SOLUTION BRIEF

Accelerating Packet Evidence for Faster Incident Response

The Packet Evidence Gap

NetOps teams are under constant pressure to resolve network and application incidents faster. Alerts, dashboards, and performance metrics can identify symptoms quickly, but many investigations still require packet-level evidence to validate root cause and determine the right response.

Since they show the actual traffic exchanged between systems, packets remain one of the most trusted sources of evidence. Packets help engineers understand protocol behavior, connection details, encrypted session activity, retransmissions, failed handshakes, tunneling, and other conditions that summary metrics may not fully explain.

The challenge is getting from detection to evidence quickly enough to keep the investigation moving. This creates a **packet evidence gap**: the delay between identifying an issue and isolating the packet-level data needed to investigate it. Closing that gap helps teams move from detection to diagnosis faster and gives engineers a stronger foundation for confident troubleshooting.

Why Retrieval Precision Matters

In large enterprise environments, packet stores can contain enormous volumes of captured traffic, but most investigations do not require every packet tied to an IP address or conversation. Engineers usually need evidence for a specific protocol, port, connection, or incident window.

That makes retrieval precision critical. Packet retrieval speed depends heavily on how much data must be read from storage before analysis begins. When searches are too broad, engineers may retrieve large amounts of technically related but operationally irrelevant traffic, slowing the investigation before the real troubleshooting starts.

By narrowing packet searches using criteria such as IP protocol and TCP/UDP source and destination ports, teams reduce the volume of traffic read from storage and reach the packets most relevant to the investigation faster. More precise retrieval helps teams focus on traffic such as:

- Specific TCP connections
- UDP-based application traffic
- Traffic over ports such as 443, 8080, or other application-specific services
- GRE-tunneled traffic
- Protocol-specific behavior during an incident window
- Client/server conversations where only part of the traffic is relevant

Greater precision reduces the time engineers spend sorting through irrelevant traffic before meaningful analysis can begin.

How AppResponse Reduces Mean Time to Evidence

Riverbed AppResponse gives NetOps teams full-fidelity packet capture, storage, and analysis for enterprise-scale networks, helping reduce Mean Time to Evidence: the time required to move from incident detection to the packet-level data needed for investigation.

AppResponse accelerates packet investigations by combining more efficient packet metadata indexing with a more direct, point-and-click search experience. Instead of forcing engineers to rely on broad IP-based retrieval or complex packet filtering syntax, AppResponse 11.24 adds more granular index criteria, including IP protocol and TCP/UDP source and destination ports, so teams can move more quickly from observed traffic behavior to the packet evidence most relevant to the investigation.

This helps NetOps teams investigate application slowdowns, degraded or failed connections, client/server communication problems, encrypted session issues, intermittent performance degradation, and network-related application incidents with less delay between detection and evidence.

By making packet evidence easier to isolate, AppResponse helps more NetOps practitioners participate in packet-informed troubleshooting. Tier 1 and Tier 2 analysts can gather relevant evidence earlier, while senior engineers and packet specialists spend less time on avoidable retrieval work and more time interpreting evidence, validating root cause, and driving resolution.

SSL/TLS Context for Faster Investigation

Faster retrieval helps teams reach the right packets sooner, but investigation still depends on understanding what the evidence means, especially when encrypted sessions are involved. SSL/TLS behavior can affect application performance and user experience, but it is harder to isolate when cryptographic context is disconnected from traffic analysis.

AppResponse brings SSL/TLS metrics into core traffic views, allowing engineers to evaluate encrypted session behavior alongside applications, host groups, client and server groups, IP conversations, and affected services. This helps teams correlate cryptographic activity with the traffic context they already use during investigation.

With this context, teams can more quickly determine whether an incident may be tied to:

- Failed SSL/TLS handshakes
- Expired or soon-to-expire certificates
- Deprecated SSL/TLS versions
- Slow handshake behavior
- Encrypted application session issues

The result is faster interpretation, less manual correlation, and stronger confidence in the evidence.

Connecting Packet Evidence to Response Workflows

Incident response rarely happens in one tool. Network events often need to be assigned, documented, escalated, or connected to ITSM and automation workflows. When packet insight stays isolated, teams still must manually move information from investigation tools into the systems where response work happens.

AppResponse helps connect packet evidence to response workflows through webhook-based alerting. Traffic Policy alerts can be sent to ServiceNow and other webhook-capable platforms, helping NetOps teams connect packet-informed insight to existing incident workflows.

This reduces manual handoffs and helps preserve context as incidents move from detection to investigation and response. Teams can move through a more connected process:

1. **Detect** the issue
2. **Narrow** the scope
3. **Retrieve** relevant packet evidence
4. **Interpret** the evidence in traffic context
5. **Trigger** or inform the response workflow
6. **Resolve** with greater confidence

The goal is not simply faster packet retrieval. It is faster incident response built on better evidence.

Keep Packet Evidence Ready

Packet-based visibility only helps when it is ready before an incident begins. AppResponse supports lower-friction operations through API-based management, system uptime visibility, and software maintenance improvements, helping teams keep packet evidence workflows available without adding unnecessary administrative drag.

For NetOps leaders, this matters because faster response depends not only on what happens during an incident, but also on reducing the operational drag that slows teams down before one begins.

Reducing Delay Between Detection and Action

Every minute spent searching for the right packet evidence can extend the time required to diagnose, escalate, and resolve complex incidents. AppResponse helps reduce that delay by giving NetOps teams faster access to the packet data most relevant to the investigation.

For IT leaders, that means more efficient incident response, better use of specialized expertise, stronger escalation quality, and less time lost between detection and action. The result is a faster, more confident path from incident signal to operational resolution.

Get Started Now

See how Riverbed AppResponse helps teams accelerate packet retrieval, reduce Mean Time to Evidence, and resolve complex incidents with greater confidence. Request a demo at riverbed.com/platform-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.