riverbed®

DATA SHEET

NPM+ for Government

Holistic network observability for Cloud, Zero Trust, and Remote work environments

The Challenge: Network Landscape is Changing and Evolving

In today's digital landscape, effective network observability has become crucial for agencies aiming to ensure seamless digital experiences and robust security. With the proliferation of remote work, cloud services, and complex network architectures, traditional monitoring tools often fall short in providing comprehensive visibility and actionable insights.

The Vanishing Network Perimeter: How It Breaks Legacy Network Visibility

Traditional network monitoring solutions, designed for data center-centric architectures, struggle to provide visibility into today's distributed IT environments. With the rise of remote work, cloud services, and SaaS applications, a significant amount of enterprise traffic bypasses the corporate network entirely, creating blind spots that legacy monitoring tools cannot address. Remote users connect directly to SaaS platforms and cloud applications, often through home networks or public Wi-Fi, making it impossible for traditional network performance monitoring (NPM) solutions to capture and analyze this traffic. As a result, IT teams lose visibility into user experience, network performance, and potential security threats outside the traditional perimeter.

The Encryption Paradox: How Zero Trust Secures—and Obscures—Network Traffic

Zero Trust networking fundamentally changes how traffic is secured and accessed, creating new challenges for traditional network monitoring. By enforcing strict identity verification and least-privilege access, Zero Trust architectures often route traffic through encrypted tunnels, micro-segmentation policies, and software-defined perimeters. While this significantly enhances security by preventing lateral movement and unauthorized access, it also disrupts conventional monitoring tools that rely on deep packet inspection (DPI) or network taps to analyze traffic flows. Encrypted connections obscure packet payloads, making it difficult to detect performance bottlenecks, security threats, or application issues using traditional methods. Additionally, with Zero Trust dynamically controlling access at the user, device, and application levels, network paths are no longer predictable, further complicating visibility.

Without modern visibility solutions that extend beyond the WAN and data center, IT teams are left in the dark, unable to diagnose performance issues or security risks. government agencies need a modernized observability strategy that integrates network intelligence across the distributed environment, enabling end-to-end visibility regardless of where traffic flows. government agencies must adopt modern observability strategies that leverage endpoint telemetry, metadata analysis, and AI-driven anomaly detection to maintain visibility without compromising Zero Trust security principles.

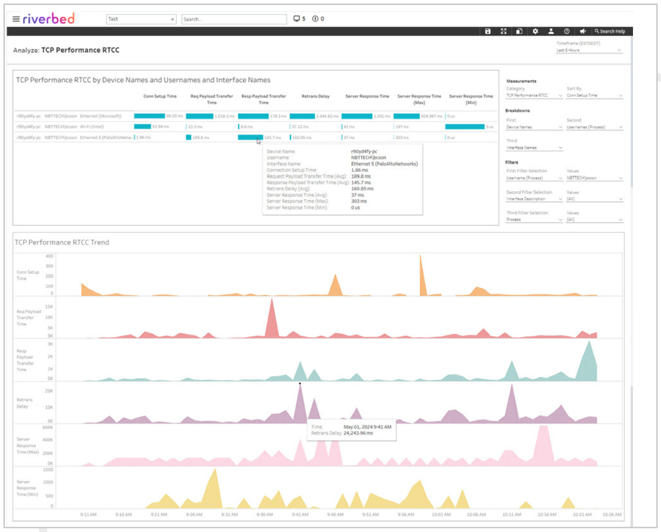
Packets: The Most Reliable Source for Network Analysis

Packets are still the optimal source for “what-did-the-network-do” analysis. How and where you collect packets has shifted though. Encryption and tunneling lowers the forensic value of captured packets using on-premises appliances, so IT need an approach that sees the data packets before they are encrypted or tunneled.

A better and newer approach is needed for visibility into blind spots. Network Operations teams:

- Cannot solely depend on appliance-centric approaches and can’t presume centralized, data center-based only will see everything IT requires.
- Need an approach that analyzes packets where the data is readily available and provides the value expected each and every time, i.e. at the endpoint.
- Require simplicity and AI-driven automation to cut through the noise and accelerate remediation.

Riverbed’s New Approach to Network Observability with NPM+ for Government



Analyze: **TCP Performance RTCC**

Timeframe (ESTSEDT): Last 6 Hours

TCP Performance RTCC by Device Names and Usernames and Interface Names

	Conn Setup Time	Req Payload Transfer Time	Resp Payload Transfer Time	Retrans Delay	Server Response Time	Server Response Time (Max)	Server Response Time (Min)
r90yd4fy-pc NBTTECH\bcoon Ethernet (Microsoft)	98.20 ms	1,018.3 ms	178.3 ms	2,946.62 ms	1,931 ms	609,987 ms	0 us
r90yd4fy-pc NBTTECH\bcoon Wi-Fi (Intel)	53.94 ms	10.3 ms	8.6 ms	37.12 ms	41 ms	197 ms	3 us
r90yd4fy-pc NBTTECH\bcoon Ethernet 5 (PaloAltoNetw...	1.86 ms	189.8 ms	145.7 ms	160.85 ms	37 ms	303 ms	0 us

Device Name: r90yd4fy-pc
Username: NBTTECH\bcoon
Interface Name: Ethernet 5 (PaloAltoNetworks)
Connection Setup Time: 1.86 ms
Request Payload Transfer Time (Avg): 189.8 ms
Response Payload Transfer Time (Avg): 145.7 ms
Retrans Delay (Avg): 160.85 ms
Server Response Time (Avg): 37 ms
Server Response Time (Max): 303 ms
Server Response Time (Min): 0 us

Measurements
Category: TCP Performance RTCC
Sort By: Conn Setup Time

Breakdowns
First: Device Names
Second: Usernames (Process)
Third: Interface Names

Filters
First Filter Selection: Username (Process)
Values: NBTTECH\bcoon
Second Filter Selection: Interface Description
Values: (All)
Third Filter Selection: Process
Values: (All)

TCP Performance RTCC Trend

Time: May 01, 2024 9:41 AM
Retrans Delay: 24,243.96 ms

Figure1: The NPM+ Core module provides next-gen network observability, delivering expert-level network and application analysis.

Riverbed NPM+ for Government, which is FedRAMP® “In Process” and an IL5 “Candidate”, provides advanced network observability solution that combines powerful modules into a single, cohesive SaaS offering. The NPM+ Core and NPM+ UC modules are currently available, while NPM+ Packet module will be accessible soon. Designed for today’s complex IT environments, Riverbed NPM+ delivers a deep, endpoint-driven approach to observability that eliminates network blind spots and enables IT teams to streamline operations, proactively resolve issues, and ensure maximum up time.

Riverbed NPM+ for Government leverages the Riverbed Unified Agent to streamline the deployment, updates, and management of supported NPM+ modules with unprecedented efficiency.

By consolidating endpoint-based monitoring into a single, lightweight footprint, Unified Agent eliminates the need for multiple, siloed agents on endpoint devices. This reduces complexity, minimizes resource consumption, and accelerates the rollout of critical observability capabilities. Ensure new features, security patches, and performance enhancements are deployed seamlessly, eliminating manual intervention and reducing operational overhead. With centralized control and policy-driven management, IT teams deploy new modules with fine-grained control, where and when they are needed. This unified approach enables enterprises to scale their network monitoring capabilities dynamically, ensuring continuous observability across client and server devices, ensuring optimal performance while simplifying lifecycle management.

Inside NPM+: Modules & Functions

NPM+ Core Module: Expert-Level Network and Application Monitoring

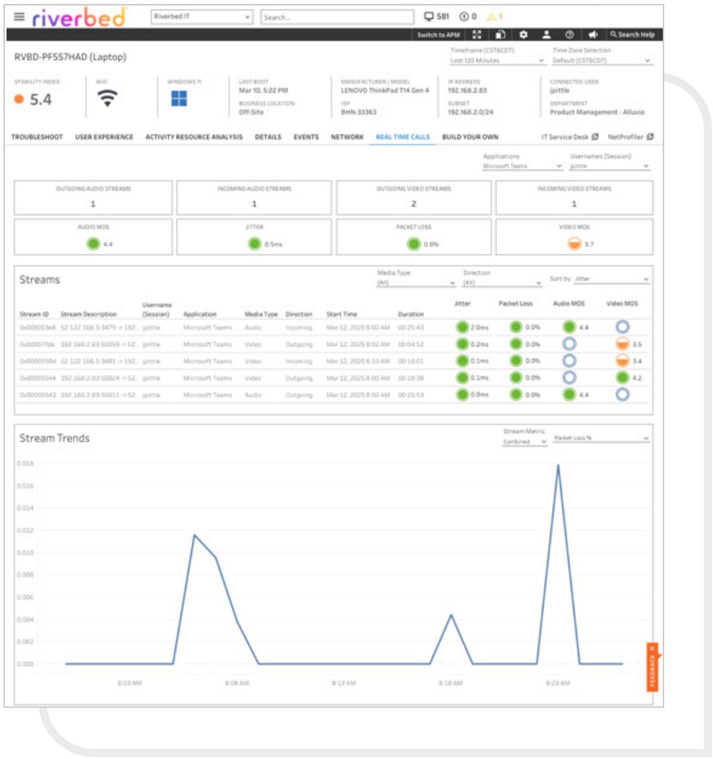
NPM+ Core Module is the foundation of Riverbed's next-generation endpoint-based network observability, delivering expert-level analysis across both network and application domains. It provides deep packet-based visibility enabling IT teams to pinpoint performance degradations with forensic precision. By correlating network telemetry with application-layer insights, NPM+ Core quickly helps IT distinguish between network and application issues and speeds troubleshooting with a wealth of network metrics, as well as client insights.

Using deep traffic inspection, the NPM+ Core ensures organizations maintain full control over their network, optimizing performance across edge, cloud, and hybrid environments. Its scalable architecture supports enterprise-wide observability, empowering IT to proactively manage service quality, dramatically reduce mean time to resolution (MTTR), and drive continuous performance improvements.

NPM+ UC Module: VoIP & Video Monitoring Without the Guesswork

The NPM+ Unified Communications (UC) Module provides real-time, high-fidelity monitoring of voice and video performance across leading conferencing platforms, including Microsoft Teams, Zoom, WebEx, Google Meet, and more. By leveraging deep packet inspection from endpoint devices, it delivers end-to-end visibility into call quality, including jitter, MOS, packet loss, and other critical metrics that impact call experience.

Advanced AI-driven analytics proactively detect and diagnose performance degradations, distinguishing between network, endpoint, and application-related issues. This enables IT teams to rapidly troubleshoot and optimize UC performance as the calls are occurring, minimizing disruptions. Comprehensive real-time and historical insights help enterprises maintain consistently high-quality voice and video communications across distributed environments.



RVBD-PF557HAD (Laptop)

Timeframe (CST6CDT): Last 120 Minutes

Time Zone Selection: Default (CST6CDT)

STABILITY INDEX: ● 5.4

WIFI

WINDOWS 11

LAST BOOT: Mar 10, 5:22 PM

BUSINESS LOCATION: Off-Site

MANUFACTURER / MODEL: LENOVO ThinkPad T14 Gen 4

ISP: BHN-33363

IP ADDRESS: 192.168.2.83

SUBNET: 192.168.2.0/24

CONNECTED USER: jpittle

DEPARTMENT: Product Management - Alluvio

Applications: Microsoft Teams

Usernames (Session): jpittle

OUTGOING AUDIO STREAMS	INCOMING AUDIO STREAMS	OUTGOING VIDEO STREAMS	INCOMING VIDEO STREAMS
1	1	2	1
AUDIO MOS	JITTER	PACKET LOSS	VIDEO MOS
● 4.4	● 0.5ms	● 0.0%	● 3.7

Streams

Media Type: (All)

Direction: (All)

Sort by: Jitter

Stream ID	Stream Description	Username (Session)	Application	Media Type	Direction	Start Time	Duration	Jitter	Packet Loss	Audio MOS	Video MOS
0x000003e8	52.122.166.5:3479 -> 192...	jpittle	Microsoft Teams	Audio	Incoming	Mar 12, 2025 8:00 AM	00:25:43	● 2.0ms	● 0.0%	● 4.4	○
0x00007fda	192.168.2.83:50059 -> 52...	jpittle	Microsoft Teams	Video	Outgoing	Mar 12, 2025 8:02 AM	00:04:52	● 0.2ms	● 0.0%	○	● 3.5
0x0000558d	52.122.166.5:3481 -> 192...	jpittle	Microsoft Teams	Video	Incoming	Mar 12, 2025 8:10 AM	00:16:01	● 0.1ms	● 0.0%	○	● 3.4
0x00005544	192.168.2.83:50024 -> 52...	jpittle	Microsoft Teams	Video	Outgoing	Mar 12, 2025 8:00 AM	00:18:38	● 0.1ms	● 0.0%	○	● 4.2
0x00005543	192.168.2.83:50011 -> 52...	jpittle	Microsoft Teams	Audio	Outgoing	Mar 12, 2025 8:00 AM	00:25:53	● 0.0ms	● 0.0%	● 4.4	○

Stream Trends

Stream Metric: Combined

Packet Loss %

Figure2: The UC Module offers real-time monitoring of voice and video performance metrics for all major collaboration platforms.

Unified Visibility

- This broad data collection capability allows NPM+ to monitor endpoints wherever they are from traditional data centers to modern cloud environments and, remote work setups, and even tunneled or encrypted Zero Trust networks.
- Unified management dashboard that consolidates views from across the network, applications and devices.

New Deployment Paradigm

- Allows customers to deploy a single visibility agent on any user or server endpoint and select the desired DEX, network, acceleration or network module
- Flexible, easy, and scalable approach to instrumentation

Intelligent Workflow Insights

- Intelligent insights to understand all aspects of network behavior
- Measure app performance for all users of your critical apps
- Extends visibility into network environments that are otherwise unattainable – public cloud, private cloud, SaaS, remote work and encrypted environments
- Break down application response time into contributing sources and launch troubleshooting of root causes
- Measure traffic by application, user, business division, and location
- Analyze historical information for trending and capacity planning
- View device metrics, such as usernames, processes, applications, system names to streamline troubleshooting

Federal-Ready Secure SaaS

Riverbed is committed to meeting the rigorous security and compliance standards required for U.S. federal agencies to adopt cloud-based solutions. The Riverbed Platform for Government, which includes NPM+ for Government:

- FedRAMP® In Process, reflecting its active pursuit of authorization under the Federal Risk and Authorization Management Program
- An DOD IL5 Candidate, signaling readiness to meet Department of Defense requirements for handling Controlled Unclassified Information (CUI) in National Security Systems

Related Product for Government

Riverbed NPM+ is tightly integrated with the following Riverbed products to create a seamless, full-stack observability ecosystem:

- Riverbed Aternity for Government provides IT and service desk teams with end-to-end visibility—linking network conditions to actual user experience. This integration helps distinguish whether performance issues stem from the network, application, or endpoint, accelerating root cause analysis.
- Riverbed AppResponse provides deep packet-based analytics, working in tandem with NPM+ to deliver enterprise-wide network observability across edge, on-premises, and multi-cloud environments.
- The Unified Agent simplifies deployment and management by consolidating monitoring capabilities into a single, lightweight footprint, ensuring easy deploy and management of NPM+ Modules across client and server endpoints.

Learn More

For more information on Riverbed NPM+, please go to riverbed.com/npm-plus.

riverbed®

MSHD-3416_RAP_GDS_US_050825