riverbed

SOLUTION BRIEF

See What Zero Trust Hides: Unlocking Network Visibility in Encrypted Environments

Zero Trust Networking Access (ZTNA) changes the rules for how IT teams monitor networks. Instead of relying on a trusted perimeter, Zero Trust requires continuous validation of every user, device, and application connection. This shift fundamentally alters the visibility challenge for IT. With users connecting from anywhere, applications delivered across cloud and SaaS environments, and traffic increasingly hidden inside encrypted tunnels, many traditional monitoring tools—built for static perimeters and centralized data centers—lose their effectiveness. What once worked for monitoring clear, predictable flows of traffic now struggles to deliver insight in a world of dynamic, distributed, and encrypted connections.

Why Traditional Tools Struggle

Zero Trust doesn't just redefine access, it rewires how networks function. Instead of predictable, centralized traffic patterns, IT now faces a maze of encrypted connections between users, devices, and applications spread across cloud, SaaS, and on-premises environments. The result is a monitoring landscape that looks nothing like the one traditional tools were built to handle. What once felt like a single pane of glass has shattered into fragmented views, blind spots, and incomplete data.

Perimeter-focused designs:

Old tools assumed traffic flowed in and out of a secure boundary. In Zero Trust, the boundary disappears.

Encryption everywhere:

Almost all Zero Trust traffic, including VPN traffic, is encrypted. Legacy tools that depended on clear text packet inspection or visible network paths can no longer "see" what's inside.

Microsegmentation:

Traffic is broken into many small, direct connections between apps and users. Tools that relied on monitoring large, flat network zones lose sight of what's happening.

Cloud and SaaS blind spots:

Older monitoring appliances weren't built to track activity across distributed, cloud-first networks and therefore struggle with getting the data they need.

Key Capabilities Required in Zero Trust

In a Zero Trust world, the biggest challenge isn't whether traffic is being inspected, it's that almost all traffic is encrypted or tunneled. This makes legacy network performance monitoring blind at the very moment visibility is most critical. To close those gaps, modern network observability must go beyond appliance-based monitoring and network taps to extend visibility to the endpoint, the edge, and the cloud, where encrypted connections begin and end.

How Riverbed NPM+ Provides Visibility into Zero Trust

This is where Riverbed NPM+ stands apart. Unlike traditional tools that go blind once traffic is encrypted or segmented, NPM+ captures data at client and server endpoints to provide:

Encrypted traffic awareness:

Because NPM+ monitors from the endpoint, it sees the traffic before it's encrypted by Zero Trust or VPN tunnels. So even in ZTNA service edges, it still records packet metadata to spot slowdowns, failures, or abnormal patterns without needing to decrypt payloads

Correlated insights with AIOps:

Since NPM+ feeds into Riverbed IQ AI driven automation, IT gets rich, actionable insights—pinpointing root causes faster, triggering automated remediations, and reducing the time and effort needed to resolve performance and security issues.

Application visibility in Zero Trust paths:

NPM+ monitors connectivity and performance all the way to cloud, SaaS, or private apps, ensuring IT gets the data they need—even when network paths are hidden by segmentation or encryption.

Endpoint-level intelligence:

By capturing data directly from endpoint devices with the Riverbed Unified Agent, NPM+ sees user and device identity metrics, such as usernames, processes, applications, and system names.

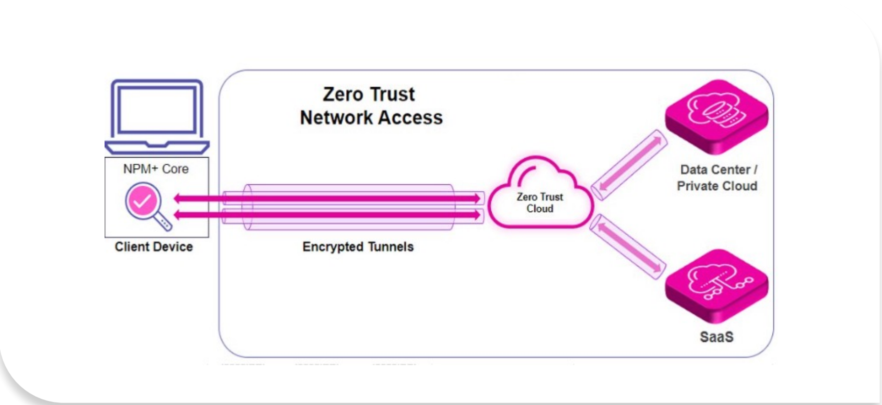

Figure 1: Riverbed NPM+ captures traffic at the endpoint—before it enters encrypted by Zero Trust or VPN tunnels—delivering full network observability into remote work, SaaS, and private cloud performance that traditional tools lose.

The Bottom Line

Zero Trust brings better security, but it makes network observability more difficult. Legacy tools that depend on clear network paths, decrypted traffic, or centralized monitoring lose visibility. Riverbed NPM+ restores it, giving IT teams the ability to see into encrypted VPN and Zero Trust connections, track performance across micro segmented networks, and ensure secure, reliable digital experiences.

Get more details on Riverbed NPM+.

> "Riverbed identified three key blind spots that NPM+ can illuminate. First, it will reveal the performance of network traffic to remote users, where there is no ability to add traditional network monitoring equipment. Second, it provides details on traffic terminating in the cloud. Finally, it provides visibility into traffic that traverses tunnels to and from zero trust network access service edges."
>
> Enterprise Management Associates

riverbed

About Riverbed

Riverbed, the leader in AI observability, helps organizations optimize their users' 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 improve 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