

Riverbed



Network Observability

The Intelligent Network Observability Blueprint

A practical path from
reactive monitoring to intelligent
network operations

riverbed®



Table of Contents

- 3. The Network Changed. NetOps Must Change with It.
- 4. What Modern NetOps Requires
- 5. The Modern NetOps Blueprint
- 6. How Network 360 Brings the Blueprint Together
- 7. Where Intelligent Network Observability Creates the Most Value
- 8. Five Priority Use Cases for Intelligent Network Observability
- 13. See Everything. Know Sooner. Act Smarter.



The Network Changed. NetOps Must Change with It.

Modern network operations have become harder to see – and harder to understand.

Applications span data centers, public cloud, SaaS, and third-party services. Employees connect from offices, homes, and virtually anywhere else. Traffic crosses Wi-Fi, ISPs, cloud networks, Zero Trust services, and infrastructure that NetOps may neither own nor directly control.

In many of these environments, the most useful observation point is no longer inside the enterprise network. Visibility increasingly must extend to the endpoint, where NetOps can see the connection as the user experiences it, even when traffic crosses networks the enterprise does not own or becomes obscured by Zero Trust and encrypted tunnels.

At the same time, network teams are managing more data, more dependencies, and more change while still being expected to answer the same fundamental questions:

- What is happening?
- Why is it happening?
- Is the network responsible?
- What changed?
- What should we do next?

Traditional network monitoring provides critical evidence for investigating performance and resolving issues. But in today's distributed environments, that evidence often tells only part of the story. Teams also need to connect information across the environment, understand how users, devices, applications, paths, and infrastructure relate, and determine what matters quickly enough to act.

Closing that gap requires a different operating model – one that combines broad visibility, connected context, and AI. Riverbed calls this **Intelligent Network Observability**.

Intelligent Network Observability applies AI across complete, connected network context to help teams understand what is happening, determine why, anticipate emerging problems, and increasingly take action before disruption spreads.

What Modern NetOps Requires

Modern NetOps teams need more than another monitoring tool or another source of telemetry. They require four core capabilities working together as a connected operating model.

Broad, high-fidelity visibility

NetOps needs multiple forms of evidence – including packets, flows, infrastructure telemetry, endpoint data, and active testing across enterprise, cloud, SaaS, remote, and Zero Trust environments.

Connected operational context

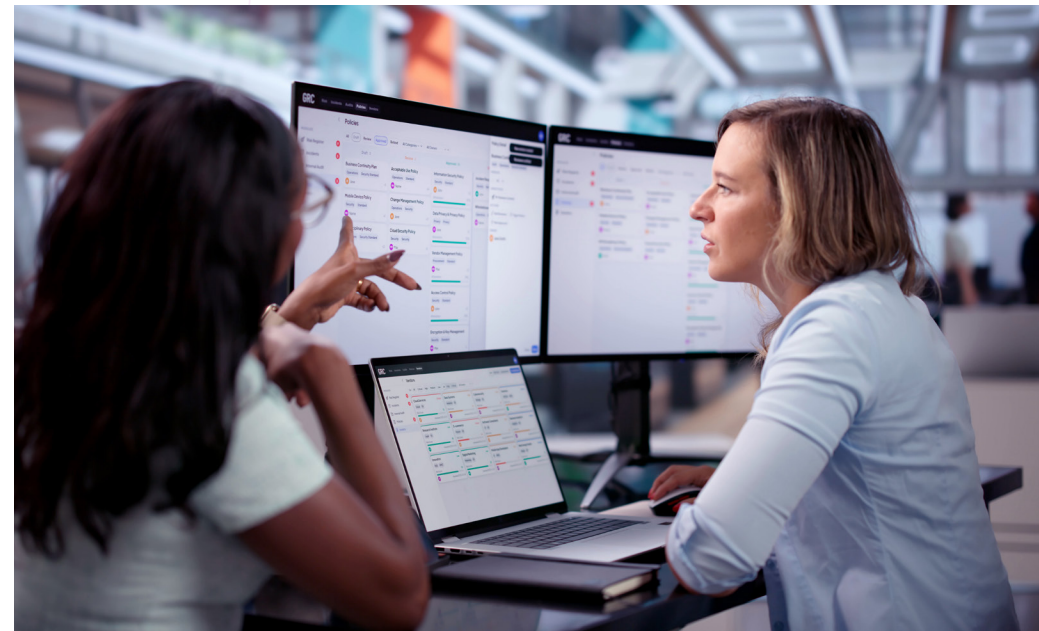
Individual signals are useful but understanding how they relate is more valuable. Modern NetOps needs to connect evidence across users, devices, applications, network paths, infrastructure, services, and events so teams and AI can understand the environment as a system rather than a collection of isolated data points.

Intelligence grounded in evidence

AI needs enough context to determine what changed, who is affected, how broadly the issue extends, what is most likely responsible, and what should happen next. The quality of those conclusions depends on the completeness and context of the evidence behind them.

A path from insight to action

Modern observability should help teams move beyond seeing and diagnosing problems toward recommending, automating, and validating trusted responses. The objective is not simply faster troubleshooting. The objective is fewer disruptions.



The Modern NetOps Blueprint

Intelligent Network Observability is not one technology. It is an operating model built from connected capabilities.



SEE

Capture evidence across the modern hybrid network

Know what is happening



CONNECT

Establish relationships across the evidence

See what is related



UNDERSTAND

Apply AI to determine likely cause

Understand why it is happening



RESOLVE

Recommend or execute trusted responses

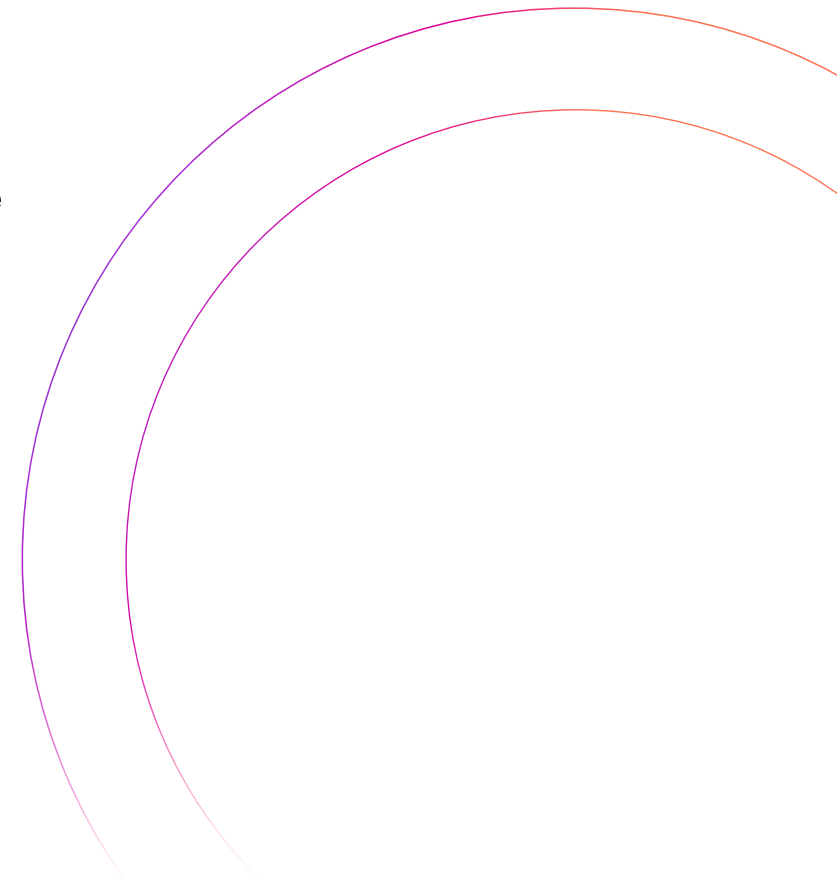
Take the right action



IMPROVE

Validate outcomes and apply what was learned

Improve the next response



How Network 360 Brings the Blueprint Together

Network 360 is Riverbed's approach for putting Intelligent Network Observability into practice. It brings together deep network evidence, broader visibility across the modern environment, a connected data foundation, and AI to help NetOps understand conditions faster and act with greater confidence. Network 360 connects all the different types of evidence NetOps already depends on and applies Riverbed intelligence across all of them.

Deep Network Evidence



AppResponse

High-fidelity packet-based network and application intelligence



NetProfiler

Enterprise-wide flow intelligence and traffic behavior

Broader Network Context



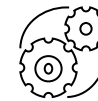
NPM+

Endpoint, remote-user, SaaS, cloud and Zero Trust visibility



NetIM+

Infrastructure health, performance, topology and dependencies



Core Assurance

Active testing of critical services, connections and paths

Connected Data Foundation



Riverbed Data Store

Connects information across Riverbed and third-party sources and establishes operational relationships among the available evidence.

Common Intelligence



Riverbed IQ

Applies causal, predictive, generative and agentic AI across connected operational context to understand conditions, determine likely causes, anticipate what may happen next and increasingly automate actions.

Conversational AI



Riverbed Q

Allows the entire team to investigate through natural language instead of knowing which tool or dashboard contains the answer.

Where Intelligent Network Observability Creates the Most Value

Intelligent Network Observability is most valuable where traditional monitoring leaves teams with incomplete visibility, disconnected evidence, or too much manual investigation.

Common starting points include environments where:

- Remote, SaaS, cloud, or Zero Trust traffic creates visibility gaps
- Engineers must correlate evidence across multiple tools or teams
- Critical services need earlier validation before users are affected
- Developing conditions are difficult to recognize before they become incidents
- Repeatable investigations consume time from experienced specialists

These are the situations where broader visibility, connected operational context, and AI can have the greatest impact on how quickly NetOps understands and resolves problems.



Five Priority Use Cases for Intelligent Network Observability

The Blueprint becomes practical when applied to the problems NetOps teams deal with every day. These five use cases show how Network 360 combines broader visibility, context, AI, and automation to change how these problems are investigated and resolved.

1 Troubleshoot Beyond the Traditional Network

Challenge

Remote and SaaS application performance may depend on home Wi-Fi, ISPs, Zero Trust services, cloud networks, and infrastructure NetOps does not control. Traditional monitoring can lose visibility across much of that path.

With Intelligent Network Observability

NPM+ extends visibility to the endpoint and across remote, SaaS, cloud, and Zero Trust environments. This evidence can be combined with packet, flow, and infrastructure intelligence to follow performance across the complete path.

Outcome

NetOps identifies where degradation begins, reducing blind spots and resolving remote-user performance issues faster.

From: Limited visibility outside the enterprise
To: End-to-end network understanding

Customer Proof

2,000+

remote users supported

“Our employees are happier because there are fewer issues with the network.”

Cyril Broussard

Infrastructure and IT Security Manager, Ingérop

2 Accelerate Root-Cause Investigation

Challenge

A performance problem may require evidence from packets, flows, infrastructure, endpoints, and applications. Engineers often have to gather that information from separate tools and correlate it manually.

With Intelligent Network Observability

AppResponse, NetProfiler, NetIM+, NPM+, and Core Assurance provide complementary evidence. The Riverbed Data Store connects information and establishes context among those sources, while Riverbed IQ analyzes relationships and helps identify the most likely cause.

Outcome

NetOps reduces manual correlation, tests assumptions faster, and identifies root cause with supporting evidence.

From: Manually connecting the dots
To: AI-assisted investigation

Customer Proof

67%

faster issue resolution

“Riverbed gives us the insight to understand issues immediately, cutting application resolution times by up to 67%.”

Galal Saad

Head of Network and Infrastructure, Faisal Islamic Bank

3 Continuously Validate Critical Services

Challenge

Traditional monitoring often detects service problems only after an alert fires or users are already affected. It may not continuously verify whether the services, connections, and paths users depend on are working as intended.

With Intelligent Network Observability

Core Assurance actively tests critical services, connections, and paths from real endpoints. When degradation is detected, those results can be combined with endpoint, infrastructure, flow, and packet evidence to determine where the problem begins.

Outcome

NetOps knows sooner when critical services are degrading, identifies where failures begin, and validates that remediation restored expected performance.

From: Wait for the complaint

To: Continuously validate readiness

Customer Proof

40+

critical applications monitored

“We can see an issue as it happens and resolve before it impacts service.”

Namık Kemal Uçkan

Head of IT Operations, Halkbank

4 Detect Emerging Conditions Before They Become Incidents

Challenge

Major incidents do not always begin with a clear threshold breach. Small changes across traffic, infrastructure, latency, utilization, endpoints, or services can combine into a developing condition that is difficult for people to recognize in real time.

With Intelligent Network Observability

Riverbed IQ applies AI across connected operational context to identify anomalies, recognize relationships among changing conditions, and surface patterns that may indicate developing risk before they become obvious incidents.

Outcome

NetOps understand what is changing earlier, prioritizes emerging risks, and intervenes before minor issues become larger disruptions.

From: Respond to visible incidents

To: Recognize developing conditions earlier

Customer Proof

Near 0

user-reported tickets

“It enables us to proactively identify and resolve potential issues before any tickets are raised, resulting in near-zero tickets.”

Ray Schumacher

Network Architect, Keysight Technologies

5 Scale Network Expertise with AI

Challenge

Experienced engineers know which evidence matters, which hypotheses to test, and which actions are safe. But that knowledge is difficult to apply consistently across the organization.

With Intelligent Network Observability

Riverbed IQ and agentic skills can capture proven investigation practices as reusable operational intelligence. Riverbed Q gives practitioners a conversational way to investigate findings, challenge conclusions, examine evidence, and determine next steps with this built-in operational intelligence.

Outcome

Organizations can apply expert practices more consistently, automate common and repeatable investigations, and allow specialists to focus on novel and higher-impact problems.

From: Expertise locked in individuals

To: Expertise applied at scale

Customer Proof

55,000

remediations every month

“That allows us to resolve issues at scale and improve productivity.”

Adam Dallaire

End User Compute, BDO Canada

See Everything. Know Sooner. Act Smarter

Intelligent Network Observability gives NetOps a more effective operating model for modern networks – one that connects the evidence teams already depend on with broader visibility and AI-driven intelligence.

It helps teams see more of the environment, understand issues sooner, act with greater confidence, and continuously improve how problems are investigated and resolved.

Network 360 brings that model into practice by combining deep network evidence, connected operational context, and Riverbed AI to help teams prevent more disruption over time.

Intelligent Network Observability defines the operating model.

Network 360 is how Riverbed delivers it. Zero Disruption is the ambition.



SEE INTELLIGENT NETWORK OBSERVABILITY IN ACTION. >



Riverbed – Empower the Experience

Riverbed is the only company with the collective richness of telemetry from network to app to end user that illuminates and then accelerates every interaction so that users get the flawless digital experience they expect across the entire digital ecosystem. Riverbed provides two industry-leading solutions: the Riverbed Unified Observability portfolio, which integrates data, insights, and actions across IT to enable customers to deliver seamless digital experiences; and Riverbed Acceleration, which offers fast, agile, and secure acceleration of any application over any network to users, whether they are mobile, remote, or on-premises. Together with our thousands of partners, and market-leading customers across the world, we empower every click, every digital experience. Learn more at riverbed.com

© 2026 Riverbed Technology LLC. All rights reserved. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed Technology. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein may not be used without the prior written consent of Riverbed Technology or their respective owners.
CS-1516_Network360_Ebook Series_101226