Riverbed

360°

Network Observability

The Future of Intelligent Network Observability is here.

Five Shifts Redefining Network Operations in the Age of AI

riverbed®

Table of Contents

For decades, the network professional has been the intelligence layer.

Network operations has become extraordinarily sophisticated.

Packets reveal exactly what crossed the network. Flows show who is talking to whom. Infrastructure monitoring exposes health and topology. Dashboards bring thousands of signals into view.

But behind all that technology, one thing has remained remarkably consistent. The tools collect and present the evidence. The network professional figures out what it means.

When an application slows, an alert fires or users start calling, experienced practitioners know what to do. Open the dashboards. Check the infrastructure. Examine the flows. Pull the packets. Compare what changed. Form a hypothesis. Test it. Keep digging until the evidence tells the story. And when the tools don't provide the complete answer, experience fills in the gaps.

That model has served network operations remarkably well. But the network around it has changed.

The network didn't get simpler. It escaped the network.

Applications that once lived in enterprise data centers now span private clouds, multiple public clouds and SaaS platforms.

Employees connect from everywhere. Traffic moves across Wi-Fi, ISPs, Zero Trust services, cloud-delivered security and infrastructure the enterprise may neither own nor control.

A single application interaction can cross multiple networks, clouds, services and dependencies before reaching its destination. And every layer generates more evidence. More endpoints. More paths. More telemetry. More dependencies. More change. More things NetOps doesn't control.

Yet when something goes wrong, the fundamental troubleshooting process remains largely the same. People still have to connect the dots.

The problem isn't that dashboards, packets, flows or network expertise have stopped working. Far from it. The problem is complexity—the volume, variety and interconnectedness of the evidence are reaching a point where human interpretation alone can't efficiently keep pace.

And network teams are still expected to answer the same questions: What's happening? Why is it happening? Is it the network? What changed? What should we do about it? Often, they are answering those questions while users are already being disrupted.

AI changes the equation.

For the first time, network operations has an intelligence layer that can work alongside the network professional.

AI can continuously examine enormous volumes of operational evidence, connect signals across sources, recognize patterns and help determine what is actually happening.

It can take on more of the work that has traditionally depended on human interpretation.

Correlating evidence. Recognizing patterns. Developing hypotheses. Identifying likely causes. Recommending what to do next. And this is only the beginning.

As AI becomes increasingly agentic, it can move beyond helping people understand a problem to pursuing an operational objective; gathering evidence, testing hypotheses, coordinating actions and ultimately helping prevent problems before users experience them.

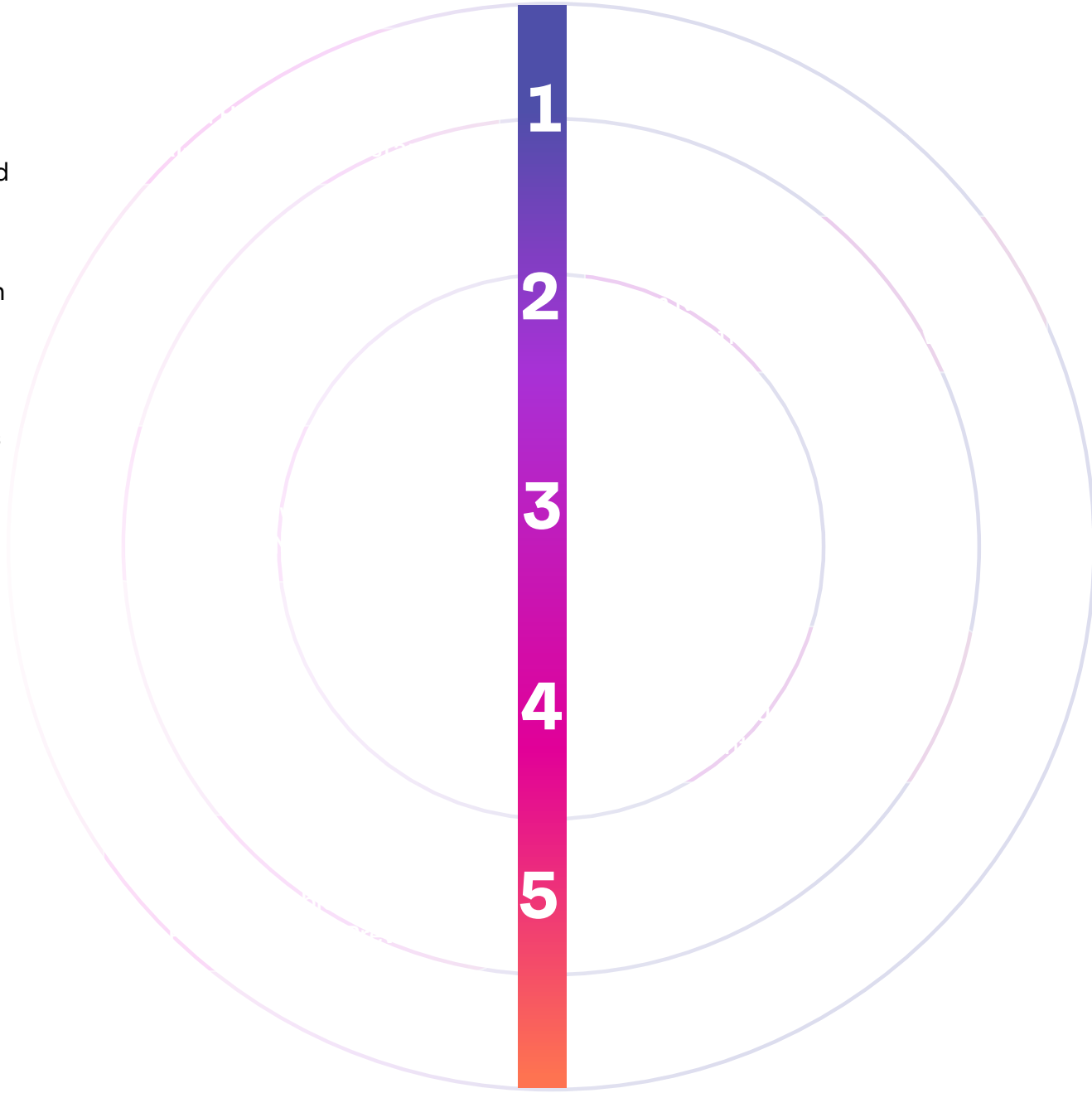
- The tools don't disappear
- The expertise doesn't disappear
- The division of labor changes

And that requires a different approach to network operations.

Intelligent Network Observability

Intelligent Network Observability is a new operating model for network operations—one in which AI works across complete, connected network context to help people understand what's happening, determine why, predict what comes next and increasingly take action to prevent disruption.

Some of that transformation is happening today. More becomes possible as AI becomes increasingly agentic and organizations become comfortable allowing it to act with greater autonomy.



Five fundamental shifts show where network operations is heading.

1 SHIFT

From Human Interpretation to AI-Assisted Understanding

Network operations has never lacked data. The challenge has been turning that data into understanding.

An alert indicates something changed. A dashboard shows where. Flow data reveals traffic behavior. Packet data provides deeper evidence. Infrastructure telemetry adds another perspective. But traditionally, it has been the network professional who brings those pieces together.

AI can increasingly take on more of that work. It can continuously analyze evidence across multiple sources, identify relationships, recognize patterns and anomalies, and develop and test hypotheses about what is happening.

Instead of simply presenting more information for the network professional to interpret, AI can help turn that information into understanding.

That changes the starting point of an investigation. The practitioner doesn't have to spend as much time assembling the evidence before applying expertise. AI can do more of the initial correlation and analysis, allowing the professional to focus on validating the conclusion, exploring exceptions and deciding what should happen next.

THE SHIFT

The network professional doesn't stop being the expert. AI helps the expert get to the answer faster.

2 SHIFT

From Navigating Tools to Investigating Through Conversation

For decades, network professionals have learned how to navigate the monitoring environment.

Which dashboard should I open? Which query should I run? Should I look at flows? Do I need the packets? Which other system might have the evidence I need?

AI creates a fundamentally different starting point. Start with the problem. *"Why is SAP slow for employees in London?"*

Intelligence can begin examining the available evidence: network behavior, infrastructure, endpoints, historical conditions and other relevant context to determine what changed and develop a likely explanation.

Then the practitioner can keep going. Why do you think it's the network? What changed in the last hour? Show me the evidence. Are all users affected? Could something else explain it? What should we do next?

Each answer becomes the starting point for the next question.

The investigation no longer has to follow the hierarchy of the monitoring tools. It follows the problem.

This doesn't eliminate dashboards or deep technical analysis. A network engineer still needs the ability to drill into a flow, inspect a packet or challenge an AI-generated conclusion.

But conversational AI changes how practitioners get there. Instead of requiring people to understand where every piece of information lives, intelligence increasingly finds and connects the relevant evidence for them.

THE SHIFT

Today, people navigate tools to find answers. Increasingly, intelligence navigates the evidence—and people interrogate what it finds.

3 SHIFT

From Network Visibility to Network Context

Giving AI access to more network data doesn't necessarily make it more intelligent.

It needs the right context.

No single source of telemetry describes network reality completely. Flows reveal traffic patterns and conversations. Packets provide high-fidelity forensic evidence. Infrastructure telemetry explains health, topology and dependencies. Cloud telemetry extends visibility into public and hybrid environments. Endpoint-based network visibility reveals what users experience across networks the enterprise doesn't own. Active testing shows whether critical services and paths are reachable and where degradation begins.

Each answers a different question. And increasingly, the evidence needed to understand a network problem may not come from the network at all.

Consider an application that becomes slow at approximately the same time network latency increases. At first, the evidence appears straightforward. Application slow + network latency high = network problem.

But endpoint telemetry shows CPU utilization spiked immediately before the slowdown. Application telemetry shows only one process is affected. Other applications using the same network path continue performing normally.

The network evidence wasn't wrong. It was incomplete.
That distinction becomes critical when AI is doing more of the interpretation.

Simply collecting telemetry in one place doesn't mean AI understands the relationships among it. It needs to know what the evidence represents, how it is connected, what changed, what normally happens and which signals actually matter.

Data aggregation is not the same as operational understanding.

THE SHIFT

The goal isn't simply to give AI more data. It's to give AI a more complete understanding of network reality.

4 SHIFT

From Individual Expertise to Scalable Intelligence

Every network operations team has people who seem to know things no dashboard can tell you.

They've seen the problem before. They know which signal matters and which one is probably a distraction. They know what evidence to gather, what questions to ask and which hypothesis to test next.

That expertise is one of the most valuable assets in network operations. It's also one of the hardest to scale.

Runbooks and knowledge bases can document what an expert knows. But someone still has to recognize when that knowledge applies, gather the right evidence and work through the process.

AI creates another possibility. What if the expertise of your best network professionals could become reusable intelligence?

Agentic skills can capture how experienced practitioners approach specific problems: What evidence should I gather? What conditions should I test? Which hypotheses should I eliminate? What sequence should I follow?

Which actions are safe?
Instead of that knowledge being available only when the right expert is available, it can increasingly be applied across the organization—consistently and at scale.

That changes the role of the expert, too. Less time repeatedly solving known problems. More time handling novel situations, improving architecture, defining policy and teaching intelligent systems how the environment should operate.

THE SHIFT

AI doesn't replace network expertise. It gives organizations a new way to capture, apply and scale it.

5 SHIFT

From Troubleshooting to Prediction and Prevention

Network operations has spent decades getting better at answering an important question:

What went wrong?

Better monitoring made problems easier to detect. Better analytics made them faster to isolate. Better diagnostic tools helped practitioners determine root cause and restore service.

AI allows network operations to begin asking a different question: What is about to go wrong?

Patterns can emerge before a threshold is crossed. A series of seemingly minor changes can indicate a developing condition. Historical behavior can reveal what's normal and what's not, and identify when today's activity is beginning to look like yesterday's incident.

AI can continuously look for those relationships in ways people simply cannot. That allows network operations to move beyond simply troubleshooting problems faster. It creates the opportunity to intervene earlier.

AI can help teams understand incidents faster, correlate evidence across sources, recognize anomalies and emerging conditions, identify likely root causes and recommend what to do next.

These capabilities can materially reduce the time and effort required to investigate network problems. But they are not the destination. They are the beginning.

THE SHIFT

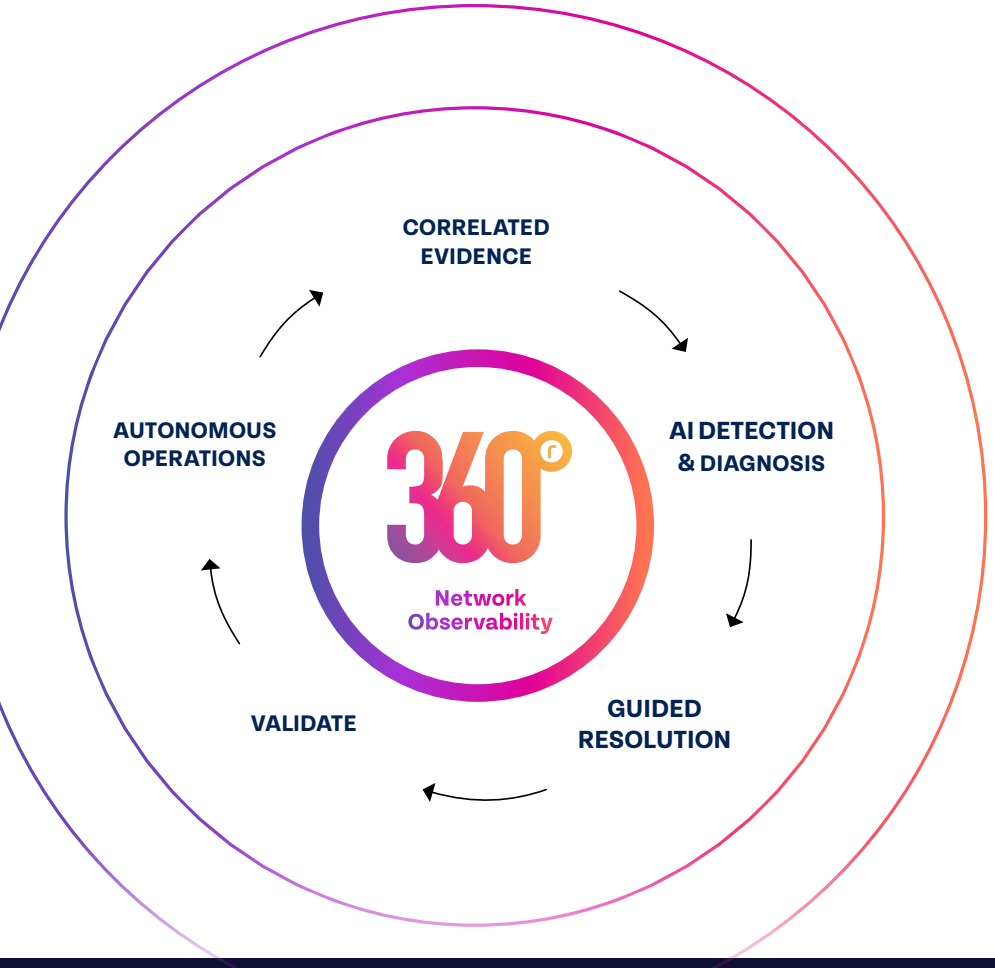
Today, network operations focuses on finding and resolving problems after they occur. Increasingly, intelligence helps teams know sooner, predict what comes next and prevent more disruptions before users experience them.

What the Five Shifts Make Possible

Individually, each of these shifts changes an important part of network operations.

Together, they change the operating model.

Together, they create the potential for a continuous intelligent operational cycle:



AI can increasingly observe conditions across the environment, understand what is happening and why, predict developing problems, recommend or take trusted action, validate whether that action worked and learn from the outcome.

As AI becomes increasingly agentic, it can take on more of that operational cycle: investigating conditions, determining what should happen next, taking trusted action and validating the outcome.

Not without people. With people increasingly supervising the process rather than performing every step. People establish the policies. People determine acceptable risk. People decide where autonomy makes sense.

Not every network operation should become autonomous. But as intelligence improves and confidence grows, more routine, well-understood and trusted processes can.

And that changes the ambition for network operations:

- The goal is no longer simply to resolve disruption faster.
- It is to prevent more disruption from happening in the first place.

That is the path toward Zero Disruption.

Making Intelligent Network Observability Real

Intelligent Network Observability defines what network operations needs to become.

Network 360 is Riverbed's approach to delivering it.
Network 360 combines 360-degree network visibility with an AI intelligence layer designed specifically for network operations, bringing intelligence directly into the way network teams investigate, understand and ultimately act on network issues.

At the center are Riverbed IQ and Q.
Riverbed IQ applies causal, predictive, generative and agentic AI to network operations, helping teams move from AI-assisted investigation to guided action, automated resolution and, over time, governed autonomous prevention.

Q provides a conversational, natural-language interface to that intelligence. Network professionals can investigate an issue by asking questions, exploring evidence, challenging conclusions and directing what happens next, all while maintaining the context of the investigation.

Behind that intelligence is the depth of network evidence required to make AI effective.

Network 360 brings IQ and Q together with Riverbed's deep packet and flow analysis, giving AI access to the full-fidelity network evidence required for deeper investigation and understanding.

NPM+ extends that visibility even further, helping eliminate blind spots created by remote employees, Zero Trust, public cloud and networks the enterprise does not own or control.

The result is a fundamentally different approach to network operations:

- 360-degree network visibility
- AI that understands the evidence
- A conversational interface for investigating and acting on it

Conclusion

Together, they give network teams a faster, simpler path from seeing what is happening to understanding why, anticipating what comes next and increasingly taking trusted action.

The future of network operations isn't about replacing the tools that got us here. And it isn't about replacing the network professionals who know how to use them. It is about changing the division of labor between people and technology.

See more. Understand more. Predict more. Automate more. Disrupt less.
That is Intelligent Network Observability.
And that is the path toward Zero Disruption.

LEARN MORE AT RIVERBED.COM >

riverbed®

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

CS-1400_Network360_Ebook Series_091526