riverbed®

WHITE PAPER

Next-Gen Network Observability

Navigating the Evolving Landscape of Network Visibility & Intelligence

Contents

In the rapidly evolving landscape of digital networks, the demand for advanced network observability solutions has never been greater. As organizations navigate through complexities brought by diverse architectures, dynamic workloads, remote work models and increasing security threats, the need for network observability tools is paramount. Modern, secure network architectures have created network performance blind spots, hindering effective observability and troubleshooting. The proliferation of critical SaaS applications and remote work has made it harder to monitor and troubleshoot end-users' digital experience. Compute resources now extend beyond data centers and hyper-virtualization and container dynamics heighten network monitoring complexity.

Additionally, to improve AI and AIOps outcomes, comprehensive instrumentation is vital, often achieved through agents that autonomously collect observability data. However, managing a growing number of agents becomes burdensome and costly, affecting system performance and user experience with manual updates, complex configuration, and potential collisions. This whitepaper delves into today's requirements for network observability, exploring the need for 'last mile' network visibility and AI-driven intelligence to advance network performance while ensuring a seamless digital experience across the enterprise.

The Evolving Network Landscape

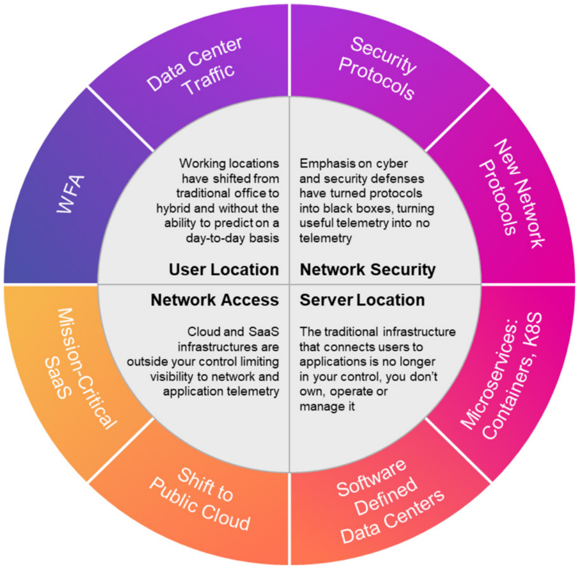
Achieving comprehensive network visibility has emerged as a daunting challenge for enterprises worldwide. The dynamic nature of networks poses new visibility gaps in pinpointing anomalies linked to performance or availability issues. With network configurations and traffic patterns shifting rapidly as part of routine operations, discerning problematic changes from normal fluctuations becomes increasingly complex.

47% of enterprises attribute reduced visibility to the rise of cloud-native applications, while **57%** cite the facilitation of remote and hybrid work, and **48%** point to the complexity of managing network performance.

Digital Enterprise Journal,
Visibility into Performance of Digital Services, July 2023

Several other important trends contribute to the complexity of running organizations today, ranging from new user locations to the evolution of new network security protocols to the decentralized structure of hybrid and complex network architectures:

- **Work From Anywhere Models:** With employees accessing cloud-based services and corporate resources from any location, whether it be a coffee shop or their home office, data center traffic has become increasingly dispersed and difficult to monitor. This dispersion not only complicates network management but also poses challenges in terms of ensuring data security and regulatory compliance.
- **Zero Trust Network Architectures:** The proliferation of new network protocols and security measures, such as SASE and SSE, further exacerbates the issue of network visibility. While these protocols enhance security by enforcing strict access controls and segmentation, they also introduce complexities in terms of monitoring and analyzing network traffic. Moreover, the widespread use of encryption or tunneling renders IT teams unable to inspect the contents of encrypted data, hindering their ability to detect and mitigate potential performance and security threats.
- **Dynamic and Scalable Networks:** The emergence of modern server technologies, including microservices, containers, Kubernetes, and software-defined data centers is enabling flexibility and adaptability of contemporary network architectures to accommodate fluctuating workloads and evolving business needs. However, the distributed and dynamic nature of these environments also introduces challenges for tracking and managing network traffic flows, as well as correlating data across disparate infrastructure components.
- **Hybrid and Multi-Cloud Environments:** The shift towards public cloud services and mission-critical SaaS applications has further compounded the challenge of network visibility. As organizations migrate their workloads to cloud environments, they relinquish direct control over the underlying network infrastructure, making it difficult to monitor and manage network traffic effectively. Moreover, the decentralized nature of cloud computing introduces complexities in terms of data sovereignty, compliance, and performance optimization.



Working locations have shifted from traditional office to hybrid and without the ability to predict on a day-to-day basis

User Location

Emphasis on cyber and security defenses have turned protocols into black boxes, turning useful telemetry into no telemetry

Network Security

Network Access

Cloud and SaaS infrastructures are outside your control limiting visibility to network and application telemetry

Server Location

The traditional infrastructure that connects users to applications is no longer in your control, you don't own, operate or manage it

The convergence of user mobility, evolving network security protocols, modern server technologies, and cloud-centric architectures has rendered it nearly impossible to understand the state of the network at any given time. To compound these challenges, as the pool of network experts proficient in analyzing diverse sets of network data, such as packet data, diminishes, the demand for automated, intelligent network insights becomes increasingly imperative.

Addressing these collective challenges requires a different strategy to network observability.

The Cornerstones of Network Performance Management

Telemetry Collection

In the realm of network observability, the diverse set of telemetry data, including metrics, traces, network flow, OpenTelemetry, and packets, forms the bedrock for comprehensive insight into network performance and behavior:

- Metrics provide quantitative measurements of network attributes such as bandwidth utilization, error rates, and latency, offering a high-level overview of network health.
- Traces offer a more granular perspective by tracking the path of individual transactions or requests across network components, facilitating root cause analysis, and troubleshooting of performance issues.
- Network flow data provides detailed information on network traffic patterns, enabling administrators to monitor and analyze traffic flows, detect anomalies, and optimize network resources.
- Packet-level data, captured through network packet analyzers, offers the most detailed insight into network activity, allowing for deep packet inspection, protocol analysis, and forensic investigation of security incidents.
- OpenTelemetry enhances observability by standardizing the collection and transmission of telemetry data across distributed systems, promoting interoperability across monitoring domains and ease of integration with observability tools.

Automated Alerting

Automated alerting mechanisms play a critical role in triggering incident response workflows. By continuously monitoring network telemetry data, these systems can detect deviations from normal behavior and trigger alerts in real-time. This proactive approach enables prompt response to incidents, minimizing downtime, data breaches, and other adverse impacts to operations.

Visualization and Analysis

Intuitive dashboards, analytics tools, and visualization techniques play a crucial role in deriving insights from network telemetry data. By presenting complex data in a clear and accessible manner, these tools enable network administrators to quickly identify trends, anomalies, and performance issues, leading to more informed decision-making and timely intervention.

By combining alerting, analytics and visualization based on ingested and processed set of network telemetry data, network performance management solutions provide views into network behavior, enabling proactive monitoring, rapid detection of issues and informed decision-making to optimize network performance.

Quick Review
09:03:19
ncome
ales:
Making Department
Film Department
Post Department
21.39%
04.55%
23.98%
65.98%
Q3
Operating Cost:
Making Department
Film Department
Post Department
Compare
Jul 2019
ENT 01
ENT 02
ENT 03
ENT 04
FA-30
SA-30
RTG-1
TB-1
T41-1
TB-1
RTG-3
TB-1
ZWT-8
TRG-324

The Shift from Network Performance Management to Network Observability

While network performance management tools have primarily focused on monitoring and optimizing performance metrics, network observability takes a broader and more dynamic approach, aiming to provide deep, comprehensive visibility and actionable insights into network behavior, performance, and security across diverse environments. Network observability also provides intelligence into the state of the network with business context. Moreover, it expands IT's ability to support enterprise-wide strategic initiatives such as AIOps and automation. While there are many reasons why enterprises invest in Network Observability, this whitepaper highlights the top ones.

Platforms that further address blind spots created by modern network architectures help organizations leap forward in gaining operational efficiencies, reducing costs, mitigating vulnerabilities, and addressing IT skills gaps. To achieve this, enterprises must use an innovative approach to monitoring environments that are otherwise inaccessible.

Top Reasons Enterprises are Investing in Network Observability

Network Optimization

Network optimization involves improving efficiency, speed, and performance by fine-tuning network configurations, reducing bottlenecks, and optimizing resource utilization for enhanced connectivity and user experience. Application performance benefits from enhanced visibility into traffic patterns and user experience, leading to better service delivery. Moreover, in cloud environments, observability tools offer visibility across distributed systems, ensuring smooth operation and cost-effective resource allocation.

Operational Efficiency

Network observability empowers network operations teams to drive proactive issue resolution and shift left with end-to-end visibility and actionable insights. With dynamic, aggregated insights and abundant diagnostic data with the right context, teams can resolve issues at the lowest possible level, avoiding escalation and additional costs associated with productivity disruptions, longer resolution time and war rooms.

Improved Security and Compliance

Automated Security Forensics: With the rising threat landscape, network observability is essential for detecting and mitigating security threats such as intrusions, malware, and data breaches. By analyzing network telemetry data, organizations can automate security forensics to identify suspicious patterns, anomalous behavior, and unauthorized access attempts, bolstering an enterprise's cybersecurity posture and safeguarding sensitive data.

Compliance and Audit: Network observability helps organizations meet regulatory compliance requirements and undergo audits effectively. By providing comprehensive visibility into network activities and access controls, organizations can demonstrate compliance with industry regulations such as Federal Information Processing Standards (FIPS), Section 508 HIPAA, and PCI-DSS, mitigating compliance risks and avoiding costly penalties.

IT Cost Reduction

Capacity Planning: Network observability solutions provide valuable insights into network traffic patterns, resource utilization, and capacity requirements. By analyzing historical data and forecasting future demand, organizations can proactively scale their network infrastructure to accommodate growth, prevent congestion, and optimize resource allocation.

Reduce Cloud Egress Costs: Network observability helps reduce costs associated with cloud egress, or data leaving a cloud environment, by optimizing data routing, minimizing unnecessary transfers, and identifying cost-saving opportunities.

Cloud Repatriation: Network observability aids cloud repatriation by identifying workloads suitable for on-premises hosting, optimizing data transfer, and ensuring seamless migration with minimal disruptions.

More AI Outcomes

AI-driven analytics in network observability deliver intelligence while enabling proactive incident detection, automated remediation, and continuous improvement. Examples of AI/ML applications include:

- Rapid issue detection and precise root cause analysis by ingesting and correlating data from various sources.
- Ingesting and processing large volumes of network data in real-time to parse, interpret, and standardize data formats from diverse monitoring tools and sources, ensuring compatibility and consistency across the integrated data sets.
- Analyzing the ingested data, identifying correlations, patterns, and anomalies that may indicate network performance issues or security threats.
- Dynamic visualization and presentation of actionable insights with the right context to facilitate proactive monitoring and analysis, allowing organizations to anticipate potential issues before they impact end-user experience.
- Enhanced accuracy by learning from historical patterns and adapting to new threats.
- Transforming narrowly defined, static automation to intelligent automation that models human decision making and logic.

> “Nearly **92%** of organizations believe AI/ ML-driven network management can lead to better business outcomes.”
>
> EMA Research Report AI-Driven Networks: Leveling Up Network Management, April 2023

The Case for Packet Analysis

Unlike other sources of network telemetry, packet analysis provides more granular insights into network traffic, allowing for detailed analysis of communication patterns and anomalies. Additionally, packets can capture data regardless of device type or location, ensuring comprehensive visibility across the network infrastructure. This approach also facilitates efficient troubleshooting by offering precise data for diagnosing issues and automation, optimizing network performance and security forensics. Experienced network engineers recognize that packets serve as the ultimate source of truth for the state of the network. Yet, many Network Observability vendors do not offer packet collection and analyses capabilities. Why? Simply put – it’s difficult.

There are a few trends that explain why packet analysis has become increasingly problematic:

Locations for packet collection have shifted, hindering network teams from troubleshooting crucial network components and leaving essential day-to-day business operations unmonitored. As outlined earlier in the whitepaper, this is because:

- Employees and customers can be anywhere.
- Compute is no longer dedicated within data centers.
- Dynamic server environments such as virtualization and container instances
- Encryption protocols obscure exactly what IT is trying to observe.

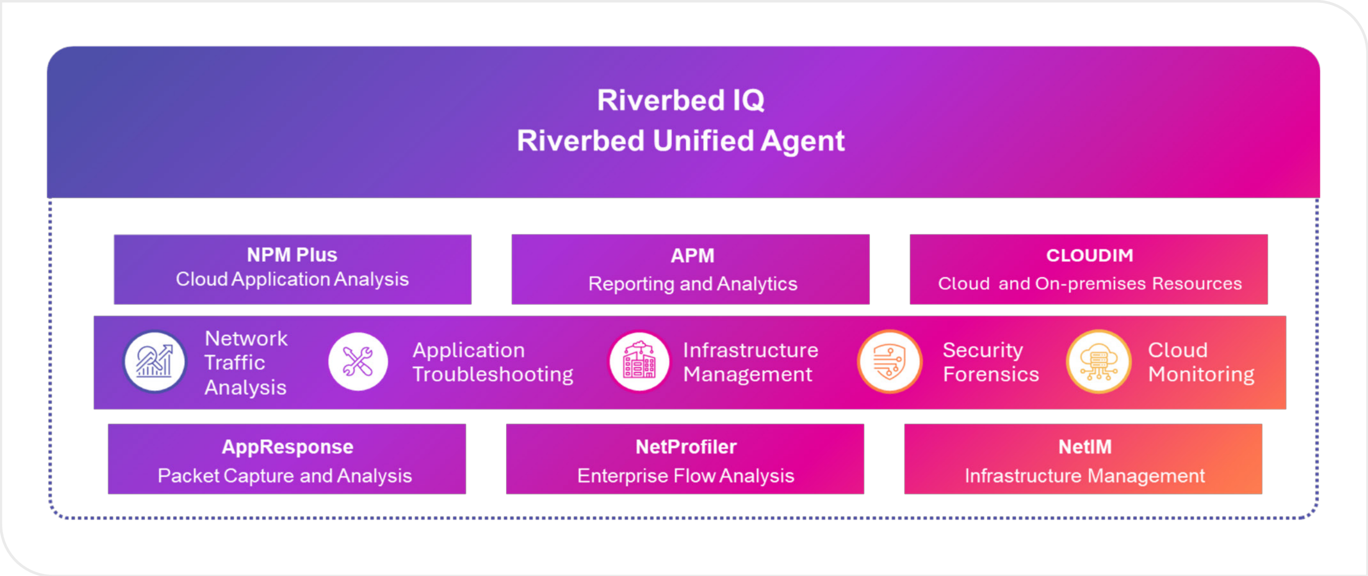
An appliance-centric deployment model is complex and costly. Appliance-based models for packet analysis are expensive and challenging to deploy primarily due to the need for dedicated hardware infrastructure, which adds to the initial cost outlay. Additionally, deploying these appliances often involves complex setup processes and may require specialized skills, further increasing deployment overheads.

The pool of "packet-heads" is shrinking. In other words, there are less expert network engineers who can manually analyze packets today. As a result, the need for automated and simplified insights is essential.

Addressing these gaps requires an innovative approach to Network Observability.

Next-Generation Network Observability Begins with Riverbed

Riverbed's Network Observability solutions include full packet capture and storage, network flow monitoring and infrastructure monitoring. Riverbed delivers transformative network observability by utilizing real-time network intelligence, processing diverse, high-fidelity network telemetry and leveraging its unified agent technology to eradicate blind spots that impede monitoring. Riverbed's visionary strategy and enabling technologies allow IT to provide the same experience to all employees in all contexts as enterprises shift from legacy network implementations to cloud-based, virtualized, and flexible architectures.



Riverbed Network Observability encapsulates the following key enabling technologies and products:

Riverbed Unified Agent

The Riverbed Unified Agent is a single agent platform for deploying and managing Riverbed and select third-party modules. As an essential element of our Riverbed AIOps platform, the optional modules are specialized for collecting different types of observability data (e.g. end user, infrastructure, packets, etc) from devices across edge, data center and cloud environments. Riverbed Unified Agent streamlines the deployment of agent modules, delivering a single installation and management process. As a result, the Riverbed Unified Agent underpins the ability to deliver enhanced digital experiences while mitigating the impact on system resources.

Packet Capture and Analysis for Edge, Data Center and Cloud Environments

With the introduction of NPM+, Riverbed establishes itself as the only AI-driven Network Observability provider offering both packet analytics and end-user experience analytics in the cloud. Riverbed takes a revolutionary step forward for faster issue detection and higher service availability while delivering a seamless digital experience.

Riverbed AppResponse

AppResponse already provides powerful, flexible network and application analytics and workflows to speed problem diagnosis and resolution. Functional out of the box with pre-defined insights and a rich variety of performance metrics. AppResponse helps IT get answers fast. It combines network forensics, application analytics and end-user experience monitoring in a single solution so IT has everything they need at their fingertips to resolve network and application performance issues quickly. AppResponse passively monitors the network and collects packet data for continuous, real-time, and historical application monitoring. Continuous packet capture means rich troubleshooting details are always available when you need them, saving time and money by minimizing the effect downtime has on business productivity and reducing or avoiding business-stopping slowdowns or outages.

Riverbed NPM+ (NEW)

Riverbed NPM+ ensures holistic network observability by extending visibility to previously unmonitored network locations. NPM+ collects decrypted data at every user and server endpoint, filling visibility gaps caused by encrypted tunnels in Zero Trust environments. Additionally, it extends the same benefits of AppResponse for Public Cloud services.

NPM+ Transforms Packet Collection

By collecting network telemetry at the endpoints, NPM+:

- Enables packet collection for previously inaccessible environments and traffic such as SaaS, public clouds, zero trust, microservices, software-defined data centers and data centers with hybrid network architectures.
- Eliminates blind spots created from remote user traffic that is routed directly to SaaS and Zero Trust environments.

NPM+ Changes the Deployment Paradigm

NPM+ is delivered through the Riverbed Unified Agent, providing a less costly deployment model than appliance or hardware-based deployment models. It also provides a flexible, easy, and scalable approach for new instrumentation via the Unified Agent, consisting of modules such as:

- NPM Core which calculates 80+ TCP/IP performance metrics
- NPM Unified Communications (UC) which analyzes voice and video packets on endpoints, delivering advanced monitoring for critical productivity apps like Teams, Zoom, and Webex
- NPM Packets which offers on-demand, continuous, and scheduled capture with filters.

It further transforms Riverbed Unified Agent into a comprehensive network activity ‘recorder’ and can easily integrate with SecOps workflows for precise forensic analysis.

NPM+ Transforms Packet Collection

NPM+ delivers simplified, easy to understand insights to understand TCP/IP connection behavior, significantly reducing the dependence on manual analysis. Its smart, interactive workflows streamline network performance root cause analysis, triage, diagnostics, and resolution across network teams. It also provides real-time visibility into network performance metrics and facilitates collaborative analysis across network operations, network engineering, system administrators, platform engineering teams, security operations and other IT stakeholders.

Enterprise Flow Analysis with Riverbed NetProfiler

NetProfiler is a flow monitoring solution that enables companies to get the complete picture of network traffic trends and bottlenecks across all data centers and remote sites. It leverages behavioral analytics to set normal network behaviors—and alert on any anomalous spikes or changes. It captures, retains and analyzes every flow received to build full-fidelity picture of your network and applications. NetProfiler can support SOAR and SIEM setups and workflows for cybersecurity solutions. Additionally, NetProfiler can be deployed anywhere and everywhere you need for on-premise, virtual, or cloud visibility. NetProfiler monitors cloud flows for Azure, AWS and Google cloud environments.

IT Infrastructure Management for Edge, Data Center and Cloud Environments

Riverbed NetIM

NetIM provides integrated mapping, monitoring, and troubleshooting for an enterprise IT infrastructure. With NetIM, IT can capture infrastructure topology information, detect, and troubleshoot performance issues, map application network paths, and diagram your network. NetIM provides agentless infrastructure component monitoring (SNMP, WMI, CLI, API, synthetic testing, and streaming telemetry) to deliver a comprehensive picture of how the infrastructure is affects network and application performance - and the user experience.

Cloud IM

Cloud IM extends Riverbed's NetIM and APM capabilities by extending monitoring into hybrid and multi-cloud environments. Key features include streamlined alert filtering, capacity planning tools, topology views such as AppNetworkPath, and Kubernetes analytics, leveraging telemetry from NetIM, APM, public cloud providers, and Riverbed's Kubernetes Operator to present a unified view of the Riverbed Platform. The visualized information can be utilized by other Riverbed services, like Riverbed IQ to provide actionable insights, offering a holistic perspective of hybrid networks for efficient issue resolution and management of cloud and on-premise infrastructure.

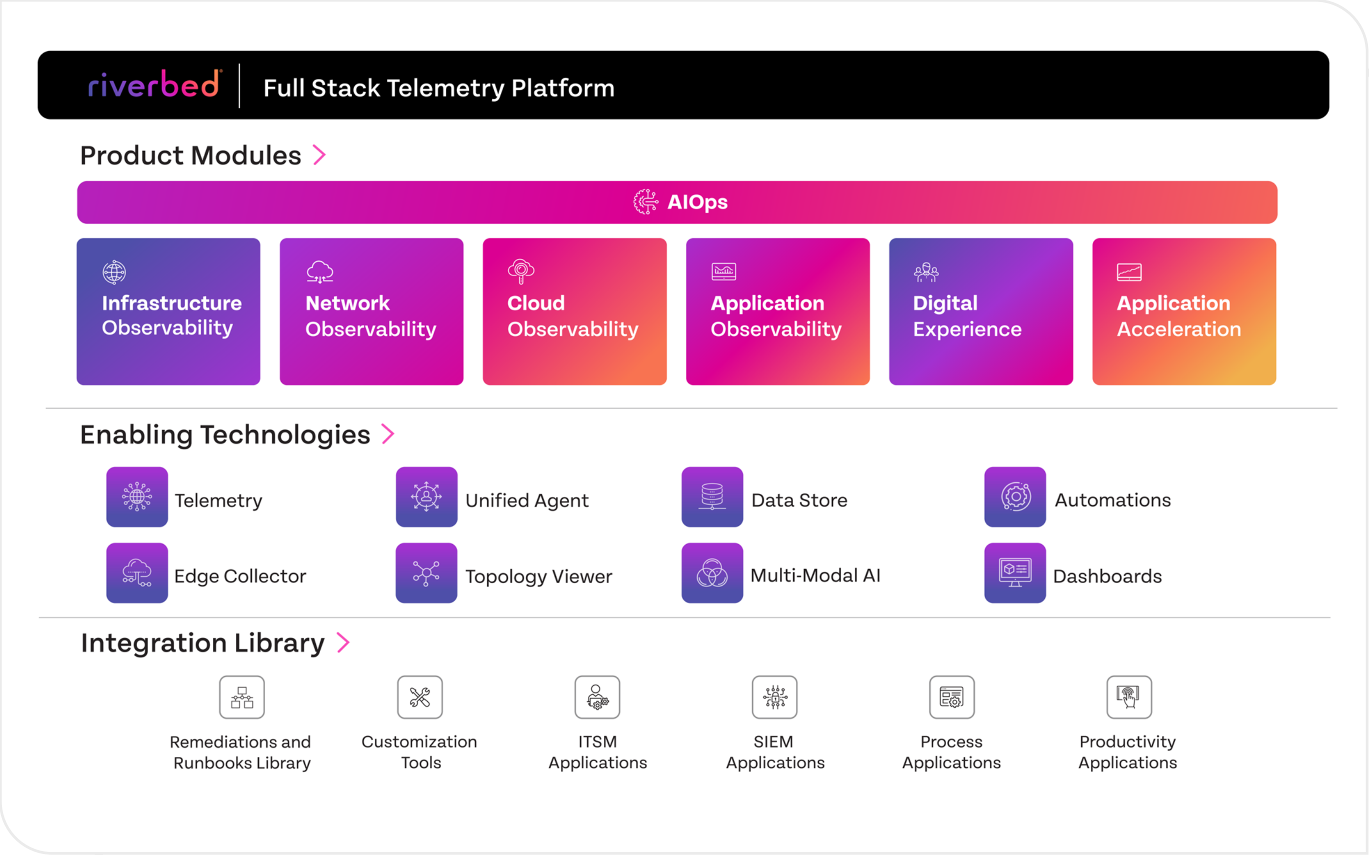
AIOps with Riverbed IQ

Riverbed IQ seamlessly integrates with Riverbed's Network Observability solutions, merges data from various observability tools and employs causal AI for pinpointing root causes, predictive AI for anticipating future issues, and soon, generative AI for offering intelligent recommendations, bolstering decision-making confidence. Riverbed delivers intelligent automation to expedite root cause analysis and resolution, with the capability to extract data from third-party solutions for enhanced diagnostic capabilities and streamlined workflows. Examples of 'Day2' network automations include Incident Response, Intelligent Ticketing, and Automated Security Forensics. It further delivers AI-powered dynamic insights and visualizations with user-centric context. Moreover, it fosters cross-silo intelligent automation with low-code runbooks that model human decision-making, automating more IT remediation steps than traditional automation solutions.

> "By 2026, **30%** of enterprises will automate more than half of their network activities, an increase from under **10%** in mid-2023."
>
> Gartner, Market Guide for Network Automation Platforms, November 2023

Riverbed Revolutionizes Unified Observability with Full-Stack, Full-Fidelity AIOps

Riverbed's Network Observability solutions are the bedrock for Riverbed's Unified Observability platform. Riverbed is the only full-stack observability platform to support infrastructure, network, cloud, applications, digital experience management, AIOps and application acceleration. It seamlessly connects all observability tools, whether ours or a third-party monitoring tool, and then applies AI (Artificial Intelligence), correlation, and automation. Together these solutions capture data across all elements of the IT landscape, including data center, clouds, and edge.



The Riverbed Unified Observability platform is defined by these characteristics:

- **Deep, Holistic Visibility:** To truly deliver a seamless digital experience, Network Observability must provide full-stack, full fidelity visibility across user experience, application, infrastructure, and network performance data for every transaction.
- **Networks without Boundaries:** Network observability tools should seamlessly operate and provide visibility anywhere, regardless of network architecture and locations. Additionally, deployment models need to evolve from appliance-based or hardware centric approaches to agent-based technology.
- **Networks of Any Size:** A true observability solution generates reliable, scalable data for any enterprise.
- **Convergence of Observability and Intelligence:** By embedding AI/ML algorithms, observability platforms contextually correlate data streams and alerts to provide actionable insights and intelligence. Intelligent automation that processes full-fidelity telemetry and ingest third party data can drive logic-driven automation and automate more work.
- **Actionable Insights Anytime and Anywhere:**
  - Real-time visibility is crucial, and a robust visibility platform must be able to perform deep-dive, protocol-level analysis and forensic evidence collection using either real-time data collection or historical data mining.
  - Tools that extract contextual metadata from data packets create a shared source of objective information that encourages collaboration across network and application teams, whether NetOps, SecOps, DevOps or AIOps.
  - For packet-level visibility data to serve as a connecting thread and a source of agility and reduced risk for IT, an observability platform must be compatible with existing security and analytics tools.
- **Ecosystem Flexibility:** A observability platform must support any combination of cloud, security, infrastructure, ITSM, AIOps or network monitoring vendors the organization has deployed in its ecosystem.

For more information, visit 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.