Top Trends in Network Observability: Heightening Intelligence, Inspection, Insights, Integration, and Innovation

Mark Leary

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Network Observability Provides the Visibility and Control Necessary to Serve Critical IT and Business Requirements

Onrushing digital business demands, continual technology advancements, and ever-improving IT practices are all applying more and more pressure on the network infrastructure and network management systems, services, and staff. Network observability solutions must provide the detailed intelligence and insights to not only assure network integrity but also focus on positive digital experiences, strengthened security posture, and fully effective IT optimization and automation.

Key Takeaways

- Understanding the state of the network at any given time, delivering consistent and high-quality network services, maximizing the productivity of both users and IT staff, protecting networked resources, and adapting readily to new requirements are keys to success in network management.

- The detailed data and in-depth analysis provided by network observability solutions should serve as contributor to management efforts across IT and foundation for both reactive and proactive automation.

- Success of network observability solutions rests on their ability to offer detailed insights into the cloud, bolster security postures and processes, deliver the best user experience, support integration with other management and observability tools, and serve to bolster staff capabilities, productivity, and impact.

Recommended Actions

- Streamline the management toolset. Leverage solutions that solve multiple functional requirements and support multiple technology domains.

- Prioritize usability and interoperability. Emphasize ease of use for multiple IT roles (e.g., NetOps, SecOps, AIOps) and ease of integration with complementary tools and data sets.

- Heighten data collection, analysis, and automation. Use multiple sources and methods to ensure complete and timely network intelligence. Apply AI-/ML-driven analytics to gain the most in-depth insights. Then, use those insights to direct automation for a more dynamic network environment.

- Move to a proactive management approach. Avoid problems. Improve utilization of resources. Enhance digital readiness. Redirect staff to strategic future-focused initiatives. Prepare. Prescribe. Protect. Predict.

Source: IDC, 2023

SITUATION OVERVIEW

In this hyper-connected digital business environment, the transformation of network architectures, technologies, and management practices to support business objectives will continue to be an enterprise and service provider imperative. Pervasive, dynamic, and high-performance networks connecting the network edge (e.g., remote workers, branches, stores, and things) and major sites (e.g., campuses, warehouses, factory floors, and hospitals) to datacenters and cloud environments (both public and private) are increasingly complex and costly. At the same time, the digital business model heightens the critical need of anytime, anywhere secure connectivity and consistent network service quality. For organizations matching limited resources and skill sets against critical and complex requirements, engineering and operating a wholly efficient and fully effective network is becoming almost untenable.

As such, networks and network teams are under tremendous pressure to keep pace with both business demands and technology advancements. All the while, expanding connectivity requirements, management toolsets, service dependencies, and security threats are complicating the design, deployment, operation, and evolution of the network infrastructure – both as a distinct IT domain and as a vital component of an entire digital infrastructure.

Enter network observability, providing detailed intelligence and insights that not only heighten network integrity and innovation but also contribute to management efforts focused on other IT domains (e.g., SecOps, CloudOps, and System Reliability Engineering) and overarching IT observability and automation efforts (e.g., AIOps). Understanding the state of the network at any given time, delivering consistent and high-quality network services, maximizing the productivity of both users and IT staff, protecting networked resources, and adapting readily to new requirements become key tenets of digital business success. All are bolstered by advanced network observability solutions.

The following top 10 list provides a view into summary takeaways from recent IDC surveys, interviews, and consultations related to network observability. These takeaways highlight defining trends in network observability into 2024 and serve as a guidebook for successful network observability solutions and practices (see Figure 2).

FIGURE 2

Top 10 Trends Driving Network Observability Advancement and Adoption

1. **Talent and Teamwork** are paramount! Usable and multipurpose tools are key.
2. **Experience** is the critical measurement — for end users, smart devices, and IT.
3. **Data** is lacking, left unprocessed, and/or locked up.
4. **Unification** drives a streamlined toolset and holistic management.
5. **Intelligence** separates robust management from remedial monitoring.
6. **Automation** should be triggered by detailed data and in-depth analysis.
7. **Predictive** approach drives continual integrity and improvement.
8. **Advancements** should emphasize security, cloud, and wireless management.
9. **Support** must match — or even exceed — technical development.
10. **Partnership** success will be determined increasingly by depth versus breadth.

Source: IDC, 2023

- **Talent and teamwork** are paramount! Usable and multipurpose tools are key. Networking staff pressures are mounting on multiple fronts – deployment, operations, optimization, innovation, and protection. And at the same time, the best and brightest of network experts are being lured away from current roles by attractive opportunities in other IT areas (e.g., security, cloud, automation) or other organizations/industries or even retirement for the most senior of network engineers and operators. Networking roles must present more exciting challenges, learning opportunities, business value, and job satisfaction. Network observability solutions must, first and foremost, boost networking staff productivity and impact – by supplementing networking staff duties and expertise and by increasing contributions of other IT staff whose efforts impact – network integrity (e.g., SecOps).

- **Experience** is the critical measurement – for end users, smart devices, and IT. The digital experience – or user experience, as some call it – is the ultimate indicator of service quality for all endpoints – human and machine. Tracking the experience of any key exchange serves to focus observability efforts on overall end-to-end performance. It is this systemwide condition that really matters to the business, given that customer satisfaction and worker productivity are top-rated digital business priorities for most organizations. And the digital experience not only serves as a bellwether of current network, application, and transaction performance but also serves as a warning for proactive management actions that head off help desk calls and user downtime.

- **Data** is lacking, left unprocessed, and/or locked up. Time and time again, survey results and IT management and staff interactions expose the significant challenges organizations face in collecting, analyzing, and sharing management data. There are many methods used to gather network intelligence, and the precision of network insights is primarily determined by processing accurate, timely, and complete data sets. Network observability solution must leverage all available mechanisms – from logs to polls to telemetry to synthetic tests – to develop a complete picture of network conditions and components. This complete picture can then be presented to the analytics engine for such processing tasks as correlations, root cause

analysis, anomaly detection, and predictive modeling. And while the complete network picture may not be needed beyond the network management area, portions of the picture certainly are useful in such areas as security management, cloud oversight, and application testing.

- **Unification** drives a streamlined toolset and holistic management. IDC's worldwide survey research indicates that observability solutions are spread wide and thin across IT functional areas. For example, only about one-half of organizations leverage observability solutions in IT operations. And that is the IT functional area that leads all others in use of observability solutions. Vital areas such as SecOps, NetOps, and DevOps lag even further behind in their use of observability capabilities. The challenges presented by this rather low level of usage within IT management domains should be troubling. But just as problematic is the challenge this presents in unifying digital infrastructure management. Whether trying to deliver the best possible digital experience to end users, the most efficient and effective digital infrastructure, or a highly productive and valuable IT organization, observability solutions should be equitably used across IT, and observability intelligence and insights should be equally and readily shared across IT domains.

- **Intelligence** separates robust managing from remedial monitoring. Measuring and displaying network conditions, while certainly helpful, provide limited gains in staff productivity and management efficiency and effectiveness. In this "passive" monitoring environment, network integrity is primarily determined by analysis and actions performed solely by the networking staff. In an "active" management environment, an analytics engine serves to offer the deep insights derived from all the data collected. So much more can be accomplished – with systems and staff – by using an observability solution that supports in-depth analysis and automated management. This not only provides much-needed relief for the operator but also delivers more precise and timely analysis and actions. And because of the voluminous data made available by the network and the complexities of network interactions and interdependencies, comprehensive data processing presents big data challenges and increasingly requires artificial intelligence (AI) and machine learning (ML). AI/ML-driven analysis not only is able to support complex correlations, precise root cause analysis, and timely anomaly detection but also enables the analytics engine to direct management actions that are learned and validated by proven use.

- **Automation** should be triggered by detailed data and in-depth analysis. IDC business value research into network automation reveals that, while some gains in staff productivity and network integrity are made by automating repetitive deployment and operations tasks, greater gains are realized by coupling analytics and automation. Without this coupling, the network operators are left to determine and execute their own actions based on the intelligence and insights presented to them by network analytics solutions. Working in concert, network analytics and automation deliver more precise and proactive management actions while improving the dynamics of the network infrastructure. Taking automation one step further, observability solutions that direct or even take actions with minimal or no operator involvement move the network closer to the level of automation available within the computing infrastructure. To date, directing problem-solving or network-optimizing actions has typically been limited to basic recommendations, at best. Solutions that move to the next level of automation – from guided remediation to full automation – differentiate themselves by not only driving staff productivity but also applying maximally effective, high-impact network management actions.

- **Predictive approach** drives continual integrity and improvement. While much of the attention on network analytics ROI focuses on reduced problem resolution times, more and more enterprises are finding that avoiding problems, accelerating digital rollouts, and properly timing network upgrades and staff redirection deliver strong value to business execution, IT service

quality, and budget control. All of these returns are driven by a move toward a more proactive and predictive network and IT management model. Key features such as precise resource tracking (e.g., integrity, usage), digital experience management, ready IT tool integration (e.g., network and application performance management and NetOps and SecOps data exchanges), and "what if" analysis allow network operators and engineers to accurately assess pending failures/slowdowns or potential capacity issues and risks.

▪ **Advancements** should emphasize security, cloud, and wireless management. While many trends dictate further observability developments, particular areas of need stand out. Recent IDC survey research indicates that the number 1 expected benefit from observability advancements is a strengthened security posture. This same survey designates gaps in cloud intelligence as the number 1 barrier to IT observability success. Network observability solutions that aid security and cloud management offer big and visible gains for IT organizations. A specific look at the network infrastructure, wireless environments are cited as the number 1 investment area for observability. For many enterprises, a wireless-first approach has been adopted for both on premises and remote access. And for service providers, 5G permeates public wireless environments.

▪ **Support** must match – or even exceed – technical development. Network observability solutions will not succeed based solely on advanced technical features. Network observability solutions provide a wealth of capabilities and require deep expertise and proven best practices to deliver to their full potential. Consultative support services focused on customer success assure the solution is properly matched to customer requirements upon initial deployment and throughout its life cycle. Proven systems integration experience and practices enable a solution to fit smoothly within the customer's current and planned network environment and, just as importantly, contribute to management tools and practices applied outside the network domain (e.g., SecOps) and overarching IT observability and automation efforts (e.g., AIOps). In addition, well-formed delivery practices aimed at bolstering such key areas as security, cloud, and automation can differentiate the great from the good solutions.

▪ **Partnership** success will be determined increasingly by depth versus breadth for solutions and suppliers. Traditionally, network performance management solutions have focused on basic connectivity and visibility within a very diverse network infrastructure, encompassing many technologies, connections, and vendors. In this environment, log processing or polling or flow telemetry provided basic network data that was "good enough" for cursory analysis. Today's networking environment requires much deeper levels of intelligence and insights – across both internal systems and external services. Supplier ecosystems are to be judged by the quality of partner exchanges and cooperation. Technical integration is growing more sophisticated, driving data collection and analysis deeper across partner tools – both systems and services. Practical integration is growing more collaborative, driving more shared responsibility for customer success and solution deployment and operation. The key here is to not judge suppliers by how many partners they have but rather by how much they do with partners that are relevant to your environment.

ADVICE FOR THE TECHNOLOGY BUYER

Network observability is driven by a who's who of industry-leading technologies and practices. Cloud services. Machine learning. Artificial intelligence. Network virtualization. Autonomous infrastructure. Real-time telemetry. Programmatic interfaces. Open source. All and more are combined to serve the complex needs of network and IT management in this digital era. Blending all the aforementioned and more into a coherent and comprehensive network observability thrust is a challenge for enterprises, service providers, and solution suppliers. The following practices are serving to drive success in network observability for IT organizations:

- **Execute as a team.** Develop an IT organizational structure, culture, practice, and skill set that is fast acting, forward looking, and team oriented. Promote observability "champions" and executive commitment. Require cross-IT support for evaluation and selection of observability tools. Use digital experience measurement as a unifying KPI.

- **Streamline the management toolset.** Leverage solutions that solve multiple functional requirements and support multiple technology domains. Network observability tools that offer intelligence and insights into LANs and WANs, wired and wireless networks, and core and edge networks deliver high value and lower costs. Network observability tools that support threat mitigation efforts drive NetOps and SecOps teamwork and a stronger security posture.

- **Prioritize usability and interoperability.** Emphasize ease of use for multiple IT roles (e.g., NetOps, SecOps, and AIOps) and ease of integration with complementary tools and data sets. Key features, such as extensible APIs, role-based dashboards, and standardized data formats (e.g., OpenTelemetry), promote data and tool sharing and provide a single source of truth across IT.

- **Heighten data collection and analysis.** Use multiple sources and methods to ensure complete and timely collection, distribution, and processing of network intelligence. Apply AI-/ML-driven analytics to that intelligence to gain the most in-depth insights into network conditions and components. Remember, the more detailed the data, the more precise the analysis.

- **Leverage analytics for action.** Tightly couple in-depth analytics and directed automation for a more dynamic network environment — one that reacts readily to changing demands and conditions. This boosts network resiliency and responsiveness, providing for a more consistent digital experience for end users and a more productive and satisfying role for networking and IT staff.

- **Move to a proactive management approach.** While there will always be a need to react to problems and threats immediately, taking a proactive approach leads to less firefighting for staff, less downtime and slowdowns for end users, less waste of networking and networked resources, and less delays in digital rollouts. Forewarned is forearmed. Prepare. Prescribe. Protect. Predict.

LEARN MORE

Related Research

- *Network Observability: Driving Big Gains in Service Integrity, Staff Productivity, Savings, and Digital Innovation* (IDC #US49928422, December 2022)
- *The Benefits of Observability in Digital Infrastructure Management* (IDC #US49679422, September 2022)
- *Worldwide Enterprise Network Performance Management Forecast, 2022-2026* (IDC #US49632922, September 2022)
- *Observability: IT Management Analytics Solidified and Unified* (IDC #US49423622, June 2022)
- *Network Analytics: Evaluating Solutions. Extracting Value.* (IDC #US48944022, March 2022)
- *Worldwide Enterprise Network Performance Management Forecast, 2021-2025* (IDC #US48122621, August 2021)

Synopsis

This IDC Perspective discusses the top trends in network observability. Onrushing digital business demands, continual technology advancements, and ever-improving IT practices are all applying more and more pressure on the network infrastructure and network management systems, services, and staff. Network observability solutions must provide detailed intelligence and insights to not only assure network integrity but also contribute to complementary and overarching efforts focused on heightened digital infrastructure resiliency. Success of network observability solutions rests on their ability to offer detailed insights into the cloud, bolster security postures and processes, deliver the best user experience, support integration with other management and observability tools, and serve to bolster staff capabilities, productivity, and impact.

"IDC research indicates that most organizations use more than 10 observability tools to measure and monitor their digital infrastructure. Many use double or triple this number! And yet, coverage gaps and blind spots continue to exist or even expand," says Mark Leary, director, Network Observability and Automation at IDC. "IT organizations need to take a more unified and streamlined approach to observability. Tools that serve multiple purposes, support multiple IT domains, and promote shared use of data drive more complete visibility and control. This leads to heightened network service integrity and networking staff productivity while reducing the cost and complexity of managing and evolving the network."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com