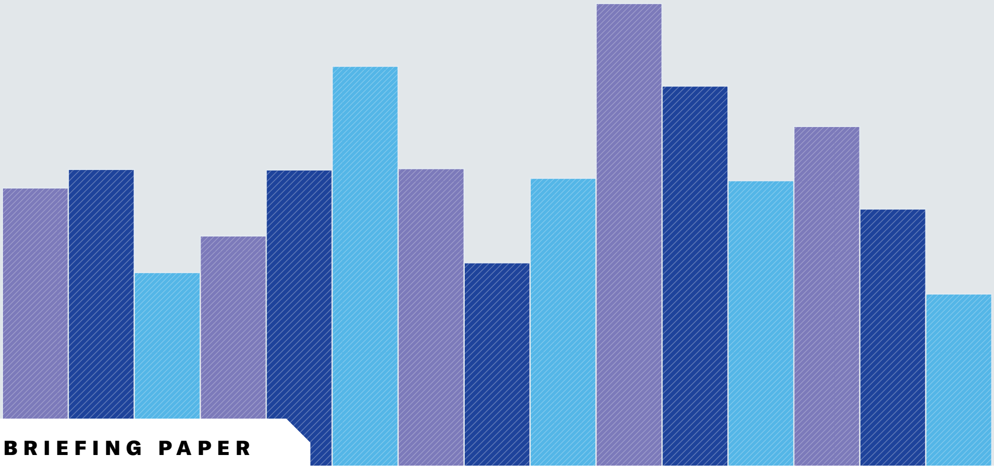
Harvard
Business
Review
ANALYTIC SERVICES



BRIEFING PAPER

Unlocking the Value of Network Observability

Sponsored by

BROADCOM

Network Observability
by Broadcom

SPONSOR PERSPECTIVE

Mike Melillo

Head of Network Observability Software

Broadcom

We're now operating in a digital world in which a strong network is the heartbeat of a thriving business. Networks support almost every critical business operation and service. Today, business performance is integrally connected to network performance—making network visibility more critical than ever before. However, as we embrace cloud services and other modern approaches, our networks have become more dynamic, multifaceted, and complex. This transformation has introduced new visibility gaps for teams in the network operations center (NOC) as well as other stakeholders, including developers, site reliability engineers, and security administrators.

The lack of complete network visibility is a major reason why operations teams struggle today. Without comprehensive visibility, teams can't quickly identify and resolve issues. They can't proactively spot potential problems and address them before they have an impact on users or the business. Fundamentally, they can't focus on what really matters, resulting in costly outages, poor service levels, reduced productivity, and lost revenue opportunities. That is why the demand for network observability solutions is rapidly increasing.

At its core, network observability is about gaining full visibility across entire network delivery paths, whether those paths reside within the data center or span hybrid multi-cloud environments. It's about gaining end-to-end views and insights, whether networks are managed by internal teams or by internet service providers, cloud vendors, or any other external entities. At Broadcom, we recognize that network teams are responsible for service delivery, yet they increasingly lack control over all the elements that shape the user experience. That's why we're intensely focused on delivering a network observability solution that empowers teams to gain the actionable insights needed to speed performance problem resolution, improve uptime, and enhance the connected experiences of employees and customers.

We sponsored this Harvard Business Review Analytic Services Report to show how network observability can enhance network performance and user experiences, promoting positive business outcomes. I hope you find this report insightful and inspiring as you advance your organization's network observability journey.

This report demonstrates how teams in the NOC have used network observability to enhance operations and ensure networks are resilient, scalable, and high performing. For example, by leveraging Network Observability by Broadcom, Fidelity National Information Systems gained full visibility into every hop along the network delivery path—including within and beyond their data-center walls, which enabled rapid identification and isolation of degradation points and root causes. With the solution, the team improved mean time to resolution. They also enhanced mean time to innocence, shielding the internal network team from finger-pointing. By speeding resolution and preventing disruptions of client services, the organization reduced costs and penalties associated with service-level agreement breaches.

Read on to discover essential approaches for optimizing network operations, accelerating network transformations, and enhancing connected experiences.

Unlocking the Value of Network Observability

Today's computer networks are often highly complex digital channels that carry data and communications that power markets, trade, and digital commerce. Failure in the form of network disruption or poor bandwidth has always been unacceptable to every network user, but it is also not uncommon. Until recently, network carriers and large enterprises could sustain uptime by relying on network monitoring tools that collect and analyze device metrics. But as networks have grown in complexity and become more widely distributed in recent years—due to the rise of cloud computing, software-defined networks, hybrid work, data analytics, and, more recently, artificial intelligence (AI)—a new generation of network observability tools has demonstrated its superiority at managing this complexity.

These network observability tools give network teams deep visibility of the entire network delivery path, especially in the cloud where the network operations team intersects with global cloud service providers known as hyperscalers. Network observability can illuminate blind spots in complex, distributed networks and clouds with tools that filter out the noise of false alerts, detect dynamic patterns, and pinpoint anomalies and performance issues—delivering actionable insights that prevent costly service outages.

"Seeing outside of our data center networks and seeing the cloud over critical pathways beyond our walls is vitally important to us," says Keith Fiala, senior systems manager at Jacksonville, Fla.-based Fidelity National Information

HIGHLIGHTS

Network observability can illuminate blind spots in complex, distributed networks and clouds with tools that filter out the noise of false alerts, detect dynamic patterns, and pinpoint anomalies and performance issues—**delivering actionable insights that prevent costly service outages**.

Before the advent of network observability tools, there was **endless finger-pointing between customers and service providers**.

While achieving automation is a long journey, that journey has advanced several steps with the maturation of observability tools, artificial intelligence, machine learning, and richer network insights.

> “If everyone has better visibility into what’s happening, they don’t falsely accuse another group of screwing things up,” says Shamus McGillicuddy, vice president of research, network infrastructure, and operations at EMA.

Systems, a global payment processing conglomerate widely known as FIS. Fiala, who is located in Chicago, says it’s not enough just to monitor traffic within the bounds of FIS’ on-premises network, considering the company processes 75 billion transactions annually, serving 20,000 clients in more than 100 countries. Equipped with a holistic view of network data spanning multiple domains, Fiala’s network team applies observability tools to solve network problems before they happen—preventing outages and slowdowns that, left undetected, would hinder their customers’ digital commerce.

Still, observability tools emerge at a time when only a minority of organizations believe their network teams have been “completely successful with monitoring and managing networks,” noted Enterprise Management Associates (EMA), a Boulder, Colo.-based market research firm, in May 2024. EMA’s biannual study has charted a steep decline from a 49% success rate in 2016 to 27% in 2022. In 2024, however, EMA says, the success rate rebounded to 42%.[1]

That organizations are recognizing that they need to look to observability tools for prevention and to generate data-driven insights isn’t surprising, given that these tools establish a single source of truth about the health of their networks and other digital infrastructure. They’ve become a bulwark against spiraling network complexity and organizational silos that inhibit healthy collaboration between teams of technology specialists. For instance, infrastructure teams commonly blame application, storage, and security issues on poorly performing networks. Consequently, network operations center specialists tend to take these accusations personally. They view observability tools as a way to gather insights about network problems—facts that settle disputes and determine a team’s next steps.

“I would say that good observability tools can fix that dynamic,” says Shamus McGillicuddy, vice president of research, network infrastructure, and operations at EMA. “If everyone has better visibility into what’s happening, they don’t falsely accuse another group of screwing things up.”

Facing new global regulatory pressure to strengthen their IT operational resilience, organizations must become more vigilant about optimizing and tracking the performance of their networks and cloud service providers. Observability tools can kick-start or augment this effort. But making the shift from network monitoring to observability demands more than a routine software upgrade. Organizations may need additional skills on hand to master observability by training networking teams to interpret observability data or hiring workers with specialized knowledge in areas such as software-defined networking, data analytics, cloud services, and machine learning.

This report will examine how network observability optimizes network-delivered services, improves organizational resilience, and maximizes the potential of data-driven decision making and digital communications. The report will also highlight how companies deploy observability solutions, practice proactive network management, and prevent IT service-related outages in order to drive successful network operations.

Toward Zero Disruptions

Despite organizations spending vast sums of time, money, and talent on preventing network outages and keeping data flowing, a June 2023 survey of chief information officers and network engineers by Edison, N.J.-based network technology firm Opengear reports that 91% of companies experience unplanned downtime at least once per quarter and 81% experience between one and four outages in an average quarter.[2] The consequences of network downtime, much like outages caused by cyber attacks, human error, or natural disasters, can be remarkably costly, with two-thirds of outages costing more than $100,000 per incident, according to Uptime Institute, a New York City-based professional services firm.[3] *Forbes* adds that outages cost up to $5 million per hour for higher-risk enterprises in the financial services or health care sectors.[4]

What makes these statistics more daunting is that, in a data-driven age, the volume of internet network traffic is rising—it grew 25% between 2022 and 2023, according to San Francisco-based network services firm Cloudflare.[5] That proliferation in internet network traffic is in no small part due to the rise of multicloud computing, the internet of things, and software as a service—all of which entail networks.

Today few companies attempt to manage every facet of building, managing, or monitoring their business networks. Instead, they turn to network service providers, because finding network skills is notoriously challenging and “cost is a significant factor" when hiring subject-matter experts, according to the report "Managed Network Services Market," published in February 2024 by MarketsandMarkets, a Pune, India-based market research company. A network services provider augments an organization's talent pool, but it may not alleviate the mounting complexity—or risk.[6]

Predicting and controlling the behavior of a complex system is a problem known as the "complexity-reliability paradox." In a nutshell, the greater the network complexity, the more likely one failure can knock the entire system offline. In practical terms, maintaining complex networks—more prone to crashes than basic ones—requires additional resources like engineering specialists and tools for diagnosing the root causes of network problems. But, in yet another paradox, finding more answers can spur even more questions.

The impact of complexity is evident in modern data networks, where the connections seem endless and the infrastructure increasingly comprises a hybrid of cloud and on-premises computing. "There's a lot of hybrid infrastructure, and people are using multiple cloud providers," explains EMA's McGillicuddy. "They might have some sort of hybrid-cloud environment with data center and public cloud footprints, and that adds complexity to configuration management and security policy." He believes inconsistency contributes to network issues because "the tools you use in a cloud environment are very different from the tools you use in your data center to manage things."

Overburdened networks become nearly, if not actually, unmanageable. Network operations teams, known as NetOps, monitor network infrastructure such as routers, switches, and the bandwidth of connections—they know how much traffic the network can carry. The teams monitor traffic patterns, including peak usage times, and learn the loads that can impair network performance. During peak congestion periods, NetOps can implement quality-of-service policies that prioritize some applications and limit bandwidth to others.

Adopting software-defined wide-area networks empowers network teams to route and prioritize traffic efficiently while automating routine tasks like configuration and troubleshooting. Yet it also creates problem-solving "visibility challenges" that impact not only performance but also network security, cautions McGillicuddy, adding that the network teams "also want to have better visibility into changes, so a bad configuration change doesn't open up a vulnerability that can be exploited by malicious actors or could lead to an error that brings down the network."

Maintaining network resilience is a complicated and, at times, high-stakes effort. High-bandwidth network services almost always come with service uptime guarantees that network service providers spell out in service-level agreements (SLAs). Organizations typically demand that their service provider provide them with a "five-nines" guarantee—meaning 99.999% uptime—which, if missed, can trigger financial penalties that the service provider must pay to their customer. In the case of "internal SLAs"—agreements between an organization's in-house networking team and its various internal business clients—the penalty may result in missed cash incentives, typically for managers. The quest to meet SLAs—and avoid penalties—can drive observability investments, just as it did for FIS.

Ninety-one percent of companies experience unplanned downtime at least once per quarter and 81% experience between one and four outages in an average quarter, according to a June 2023 survey of chief information officers and network engineers by Opengear.

Among its other financial services endeavors, FIS is a large cloud services provider—running a complex global network—so it could be susceptible to making penalty payments if it doesn't meet SLA guarantees. FIS began developing a network observability solution in 2021, and by late 2022, the first iteration was published, recalls Fiala, the senior systems manager. "Now that it's further deployed throughout the enterprise, we're in a better posture with our oversight of things," he says.

Observability enables Fiala's team to monitor the present and keep an eye on the near future. "If a network device goes down, there's an impact" on the network service, he says. "But if there's any indication that the device is struggling, that's what we'd like to see through observability so we can be proactive and remediate issues. That aligns with the goal of our company, which is zero disruptions to our client services."

Mean Time to Innocence

Before the advent of network observability tools, there was endless finger-pointing between customers and service providers. "We ran into painful troubleshooting bridge calls with multiple folks trying to figure out where the problem lies," says Fiala. "We've had third-party partners point fingers at us. That's why it became critical for us to have observability, see outside of our managed space, and point to where the existing

> “We’ve had third-party partners point fingers at us. That’s why it became critical for us to have observability, see outside of our managed space, and point to where the existing issue lies,” says Keith Fiala, senior systems manager at Fidelity National Information Systems.

issue lies.” FIS’ ability to “provide evidence” made a difference in resolving these disputes, he adds. “That’s the real key.”

As with many monitored operational tasks, network teams track their performance in myriad ways, most notably through keeping an eye on uptime and availability, but also by recording critical metrics such as mean time to remediation, SLA compliance, and bandwidth utilization. Unquestionably, however, the measurement that’s nearest and dearest to network teams is known as mean time to innocence (MTTI), the average time it takes to prove that a problem is not their problem. Despite this description, the teams aren’t shirking responsibility, as the proof of innocence involves gathering irrefutable evidence and running tests as needed. Unresolved ownership of an error may prolong repair and recovery, which leads to dissatisfied customers and, ultimately, unhappy shareholders.

MTTI is a vital step for FIS, which guarantees service uptime to its 20,000-plus customers and is on the hook for unavailable networked services. Fiala’s team sends “traces”—which can track the journey of a request or transaction across a network—and metrics from networking monitoring and logs in to the observability platform. “We can provide evidence to third-party partners that this issue is on their side and we need someone deployed and troubleshooting quickly,” he explains.

The traces Fiala mentions are among a mixed set of digital inputs known as telemetry, a critical if unheralded component of observability’s success. “It’s just about collecting data from more places in different ways to improve visibility,” he explains. “Places that network teams don’t have good visibility right now.” For example, his team may send a trace that might record the time it takes for a request to cross a network, note errors, and track resource usage. Fiala’s team may check syslogs (system logs) and deploy traces plus what he calls synthetic transactions that model how applications may perform under stress.

In theory, synthetic data enables network teams to improve their predictive capabilities by modeling a scenario that doesn’t exist or hasn’t yet occurred in their actual data. But it may not be for everybody. “Synthetic data is great, but it’s based on models and projections,” not actual data, emphasizes Will Townsend, vice president of Moor Insights & Strategy, a market research and advisory firm based in Austin, Texas.

Rather than using synthetic data, Townsend thinks companies should use “data that are relevant to their industry, relevant to their workload needs. It’s inherently going to be a more accurate predictor of network performance and security performance. The disadvantage [of synthetic data] is you don’t get the same level of accuracy that you do with real data.”

Seeing What’s Ahead

Automation is a long-standing overarching objective of network management. In theory, the greater the process automation, the more efficient the action, from both a cost perspective and a productivity perspective.

While achieving automation is a long journey, that journey has advanced several steps with the maturation of observability tools, AI, machine learning, and richer network insights. One form of automation that will make a difference is AI that detects network anomalies and then recommends “what you should do in response to [them],” McGillicuddy says. “That’s where people are starting to invest money now.”

According to FIS’ Fiala, “AI has been a transformative technology in our space.” He believes AI can help monitor issues beyond their data center walls. Identifying a trend and determining that it may need additional bandwidth can prevent a “situation from happening on the network that is outside the norm. Is this [problem] just a one-time spike that went up and will come down, or will it grow over time and have an impact on our services?”

The answers to Fiala’s questions may require richer data sets. “Well, it’s critical. Data improves models,” explains Moor Insights’ Townsend. “A lot of what you’re seeing with observability is the more telemetry you have, the better. Better data is going to lead to better outcomes.”

One of the better outcomes includes self-healing networks, so called because such networks have the ability to automatically detect, diagnose, and resolve various issues without real-time human intervention. Observability provides critical inputs such as predictive analytics to forecast impending performance or equipment problems. “We can proactively prevent disruptions or impacts to our client services,” says Fiala. “Where possible, we want to use AI in our operations in self-healing areas.” The objective, he says, is to “reduce our mean time to resolution for network events.”

“A lot of what you’re seeing with observability is the more telemetry you have, the better. Better data is going to lead to better outcomes.”

Will Townsend, vice president,
Moor Insights & Strategy

A Tool for Building Bridges

Each of the handful of ops, or operations, teams that manage digital infrastructure selects its primary domain management tools. In practice, this circumstance means that while network specialists may favor a particular monitoring or observability tool, security teams may embrace a similar product from one of their preferred software vendors. Though the tools may process similar telemetry, each tool's dashboard is tailored to the preferences of the team—development, networking, data management, or security—that will be using it

Townsend believes that some network visibility problems are caused by a proliferation of vendors and tools, leading to a "bolt-on mentality. It creates gaps. It creates poor visibility and creates poor management. When you use multiple dashboards, you have to figure things out, and ultimately, it makes networks less secure."

Can observability tools reduce the proliferation and build bridges between various infrastructure teams? Townsend says that organizations are interested in the belief that by "more fully integrating networking and security, you can drive better outcomes and improve visibility. Observability can play a very important role in identifying orphaned assets on networks and raising the level of visibility of potential threats, soft spots, and gaps."

McGillicuddy says he often questions infrastructure teams about whether they're considering a tool convergence. "'Do you see value in networking and security teams sharing a network observability tool?'" he says he asks. "They say yes." Then he says he asks: "'Do you see any barriers to doing it?' They say yes."

Though tool convergence may not be imminent, information sharing is becoming a priority, at least for networking teams. In the EMA study, respondents cited security risk reduction (36%) and improved network visibility (34%) as the most important concepts for measuring the success of the network management team. **FIGURE 1**

"A security team will often know that there is value in what is contained in the network operations team tools," explains McGillicuddy, who believes that security teams may tap into observability tools, perhaps with a dashboard. Enhancing the productivity of infrastructure teams may also generate value. "If your people can reduce the amount of time they spend on a typical task and you can save three hours of their day or 10 hours of their month by deploying a better tool, that translates into a lot of money."

Conclusion

As organizations gain awareness of blind spots in their networks and cyber defenses, observability tools stand ready to detect issues and identify the root cause of current or impending problems. Observability is catching on in other infrastructure fields, such as data storage and enterprise applications. In the EMA study, improved network visibility emerged as a strategic goal, McGillicuddy points out. "So, they started to align their overall strategy for network observability around things like public cloud and software-as-a-service applications," he says about the respondents.

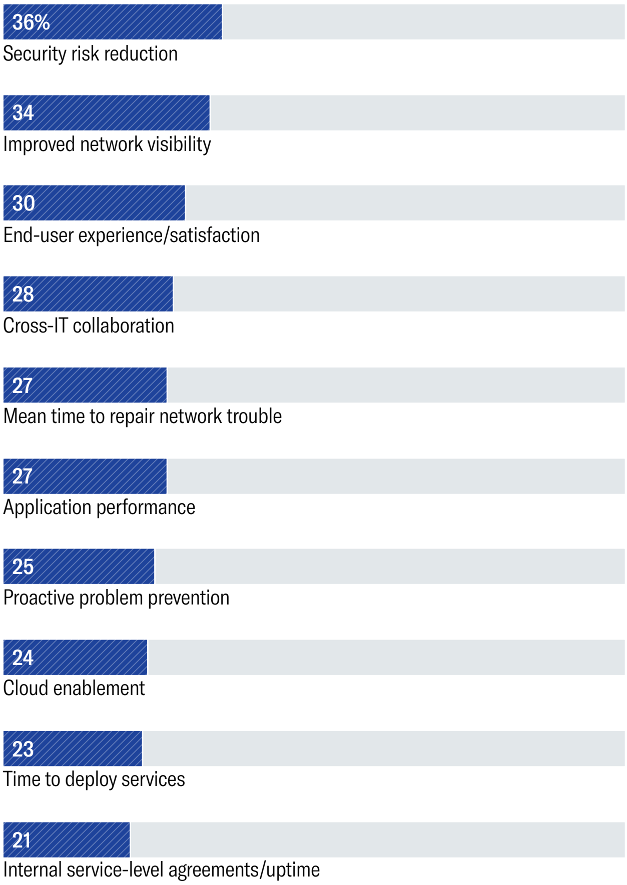
Simplifying observability and automating processes will help popularize this powerful new class of tools. "Making this platform usable for people that aren't data scientists" was one of FIS' primary objectives in deploying its network observability tools, says Fiala. The return on investment includes money saved by not having to pay out SLA downtime

FIGURE 1

Measuring Success

Networking teams are judged by risk reduction and improved network visibility criteria

Which of the following concepts is most important for measuring the success of the network management team?



Source: Enterprise Management Associates survey, May 2024

“If your people can reduce the amount of time they spend on a typical task and you can save three hours of their day or 10 hours of their month by deploying a better tool, that translates into a lot of money,” says EMA’s McGillicuddy.

> "As observability starts to provide more value and be used more efficiently by our people, think about how much we'll save with contractual SLAs when we prevent client service disruptions," says FIS' Fiala.

penalties. "As observability starts to provide more value and be used more efficiently by our people, think about how much we'll save with contractual SLAs when we prevent client service disruptions," he says.

Observability tools not only excavate previously unavailable network data but also help organizations generate meaningful predictive insights that transform network management. "Bringing all of that information together is where we're going; it's what observability is," says Fiala, noting that the resulting data and observability tools power a practice he calls "virtual network assurance—seeing the true health state of those environments. It's going to transform the way most companies manage and maintain their environments."

Endnotes

1 Enterprise Management Associates, "Network Management Megatrends," May 2024. https://www.enterprisemanagement.com/research/asset.php/4466/Network-Management-Megatrends-2024:-Skills-Gaps,-Hybrid-and-Multi-Cloud,-SASE,-and-AI-Driven-Operations

2 "Opengear Research Shows Why Investment to Reduce Downtime Must Be Targeted," *Opengear*, July 2023. https://opengear.com/blog/opengear-research-shows-why-investment-to-reduce-downtime-must-be-targeted/

3 "Network Connectivity Issues Are Leading Cause of IT Service Outages," *Network World*, April 2024. https://www.networkworld.com/article/2079815/network-connectivity-issues-are-leading-cause-of-it-service-outages.html

4 Flower, David, "The True Cost of Downtime," *Forbes*, April 2024. https://www.forbes.com/councils/forbestechcouncil/2024/04/10/the-true-cost-of-downtime-and-how-to-avoid-it

5 Belson, David, "Cloudflare 2023 Year in Review," Cloudflare, December 2023. https://blog.cloudflare.com/radar-2023-year-in-review/

6 MarketsandMarkets, "Managed Network Services Market," February 2024. https://www.marketsandmarkets.com/Market-Reports/managed-network-services-market-901.html

Harvard Business Review
ANALYTIC SERVICES

ABOUT US

Harvard Business Review Analytic Services is an independent commercial research unit within Harvard Business Review Group, conducting research and comparative analysis on important management challenges and emerging business opportunities. Seeking to provide business intelligence and peer-group insight, each report is published based on the findings of original quantitative and/or qualitative research and analysis. Quantitative surveys are conducted with the HBR Advisory Council, HBR's global research panel, and qualitative research is conducted with senior business executives and subject-matter experts from within and beyond the *Harvard Business Review* author community. Email us at hbranalyticservices@hbr.org.

hbr.org/hbr-analytic-services