IBM **Cloud**

Modernize your network observability

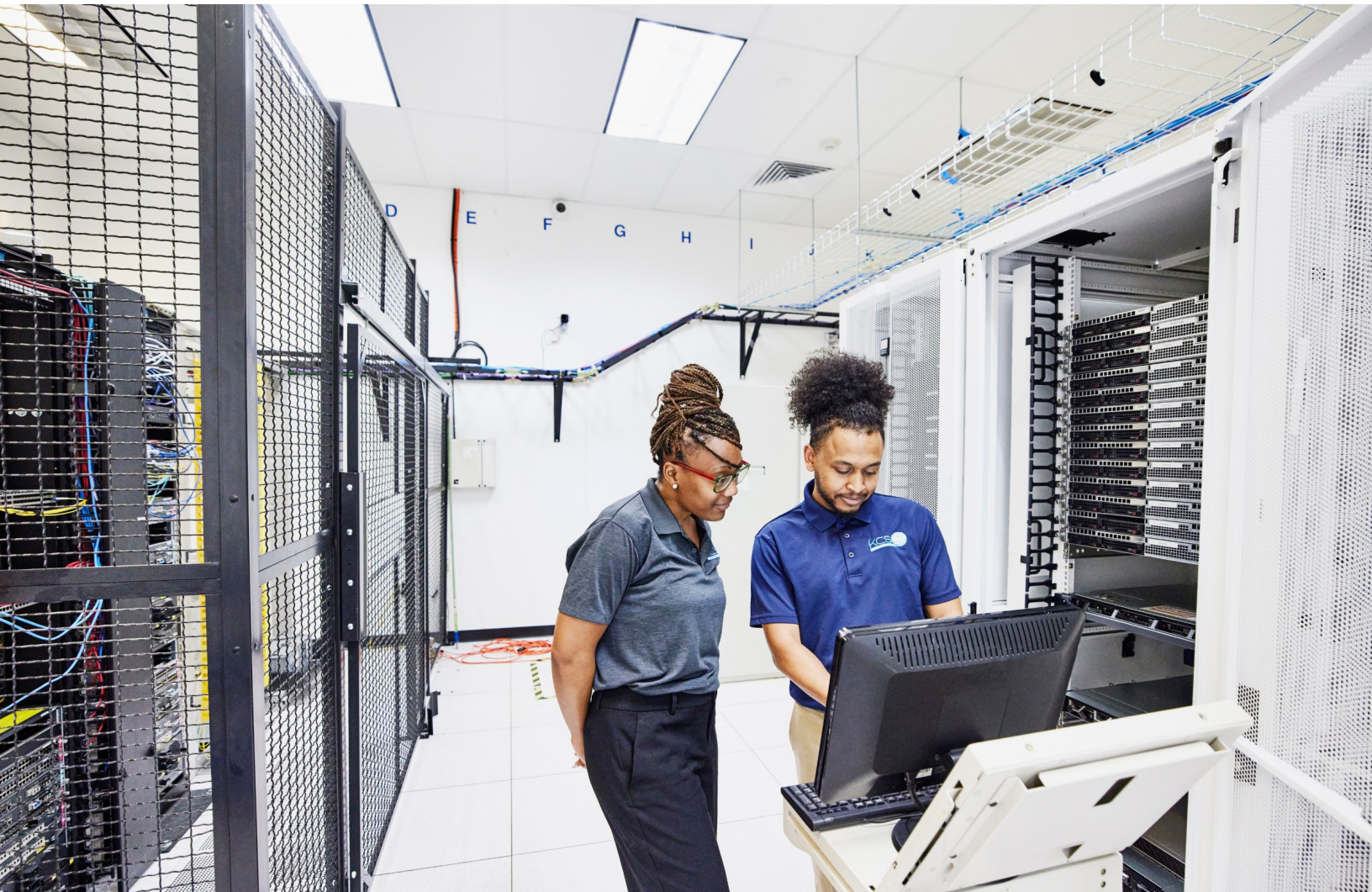

Table of contents

Introduction

Be a network hero. Help deliver faster and easier ways to find, use and share performance insights in your organization.

Network observability has never been easy, but it has become far more difficult as the complexity of IT infrastructure has soared.

Part of the challenge is the huge amount of performance and management data now being generated by growing networks. Another factor is the evolving nature of access to network performance data. Teams are rearchitecting their networks to accommodate the latest in wifi, software-defined networking, multicloud, software as a service (SaaS), virtualization, 5G and other technologies.

To keep up, network observability systems must be able to collect and analyze data from software-defined control systems and their associated virtual instances and physical devices—and from traditional network resources—at the same time. Further complicating this challenge are entirely new types of network "devices" such as virtual routers that are being provisioned and are in turn producing new types of network data and new ways that data flows throughout the environment.

All the performance data now being generated for devices and their key indicators needs to be monitored continuously, analyzed quickly and accurately, and when necessary, acted upon rapidly. Doing so with modern networks requires equally modern observability approaches.

Yet many networking teams at enterprises, communication service providers (CSPs) and managed service providers (MSPs) are still trying to do the job with outdated tools and approaches. They struggle to gain accurate insights from their network data and use them effectively. They struggle in taking automated actions based on insights, often due a lack of trust of the data. As a result, their operational efficiency around network observability is nowhere near where it could and should be.

This need not be the case. There are steps that networking teams can take to increase their operational efficiency and effectiveness. Because "you can't manage what you can't see," it starts with establishing solid network coverage with comprehensive data collection. Once that foundation is established, teams can take the next steps: using analytics, adding context, building reusable content and leveraging automation workflows

This white paper outlines steps, all of which are enabled by combining comprehensive network monitoring with intuitive ways for users to work with data to gain valuable and actionable performance insights. With those insights, NetOps and IT teams can provide the consistent, reliable delivery of high-quality network services and applications their organizations depend on today. This white paper provides a roadmap for getting there.

Step 1: Build a foundation with comprehensive coverage
The basic task at hand for NetOps and IT teams is to ensure their networks, and the services and applications that run on them, are working properly. In our highly complex networks, however, things sometimes just get jumbled or simply break. When that happens, NetOps and IT team members shift into the pressure-packed part of their jobs: identifying, locating, diagnosing and fixing problems quickly. In other words, it's on these teams to deal with network issues before they trip up too many users and bog down the business.

Many teams are still managing hardware-centric data centers with physical rack-mounted servers, routers and switches hardwired with traditional WAN links based on Multiprotocol Label Switching (MPLS) and so on. Thanks to digital transformation initiatives, they're now also responsible for managing a whole new networking world. That world includes things such as virtualized network services; SaaS and cloud-based architectures that draw on network resources not on premises but out in the ether somewhere; software-defined WANs; next-generation wifi and more.

In these new virtualized, cloud-based and software-driven environments, different things happen, and they happen very quickly. Trying to monitor and manage new infrastructure with a traditional network monitoring system presents many challenges. Designed mostly for yesterday's networking requirements, those systems struggle to keep up with today's faster and more dynamic networks.

That said, transitions from heritage to new network environments rarely happen overnight. Instead, organizations, especially large ones, take a measured approach and make the transition over time. That sets up the situation in which an organization is running two separate network environments simultaneously. In those scenarios, it's highly advantageous to have a monitoring system that can straddle both environments.

Given the topic of this white paper, however, we will keep its focus on monitoring requirements for modern networks. That must-have list includes monitoring capabilities that are just as dynamic, flexible and scalable as the new infrastructures they need to watch over.

But what does that mean, exactly? Well, for openers, it must be able to handle all of the classic monitoring tasks with hardware-based devices, Simple Network Management Protocol (SNMP) polling, device flows and so on. Beyond that, a modern network monitoring system must be able to collect network and infrastructure metrics from any source—network functions virtualization (NFV), software-defined networking (SDN), software-defined wide-area network (SD-WAN), next-gen wifi, backhaul, 4G/5G and more—regardless of the size or scale. It must be capable of managing the thousands of different device types that might be present in the network. And it must have the flexibility to quickly add support for new device types as they emerge through a self-service data ingestion process.

In short, the monitoring solution must be able to collect every performance metric available from the network and digital infrastructure and integrate those metrics with flow, and log data. These capabilities and the comprehensive coverage they deliver give NetOps and IT teams a foundation of visibility that is an absolutely critical first step to the rest of this process.

Readers who have digital transformation projects that depend on traditional monitoring systems are rethinking their strategies. Slow polling of some fraction of the devices on today's networks is a surefire way to make those projects fail, with potentially catastrophic results. Modern monitoring for modern networks is the answer.

Once a team has conquered this first step and can collect all the varied types of data available in the environment with speed at scale, it's ready to tackle the next challenge: making it easy for any technical staff member to make sense of the data. This must extend beyond the seasoned network gurus who are intimately familiar with the characteristics, behaviors, and upstream and downstream relationships of every device in their environments.

It has to be easy for users to be able to quickly see and understand what the data is telling them. That comes with purpose-built analytics. They also need to be able to determine what to do about the insights provided by data and analytics. That comes with customizable visualizations. Last, they need fast and easy ways to confirm the best course of action for issue resolution. That is unlocked by reusable problem-solving workflows.

These are the key capabilities that must be in place for NetOps and IT teams to increase their network monitoring operational efficiency. Each of these areas is described in more detail in the following steps.

Step 2: Use application-centric analytics to better understand performance data

Every network observability solution enables a network operations center (NOC) staff member to look at a particular device such as a core router and then create a report showing, for example, that router's memory usage. But that report, in and of itself, is not very useful, especially if the particular staffer doesn't happen to be familiar with that device.

Let's say the report shows that there has been a sharp increase in memory usage by that server over the past 24 hours. Is that normal behavior? Is it within an acceptable range? Are things good, bad or about to get ugly? The NOC person, who is filling in for an expert colleague who's out sick or on vacation, looking at that single report, has no idea whether the situation is OK or about to become catastrophic.

For all NetOps and IT staffers to fast-forward into a position of awareness, and do so with minimal burden, they need to be able to overlay lots of different analytics policies over whatever device, object or indicator they're interested in or concerned about. Let's consider some examples.

A good starting point is if the monitoring system lets users quickly call up baselines for the device in question. Baselines, of course, represent what the system perceives as normal—the historical view of what activity has looked like for that device. With such a baseline, users can quickly compare historical versus current activity to get an initial sense of whether the memory usage spike is a regular occurrence or an outlier that spells trouble.

Further clarity can come, for example, from the ability to easily generate standard deviation reports for key performance indicators (KPIs) for any device or object indicator. Being able to easily define standard deviations lets users quickly see how much an indicator is deviating from its normal range. That increases users' awareness without adding burdensome and time-consuming tasks—one of the keys to boosting operational efficiency. With minimal effort, the user becomes aware that something specific about a device looks good—or is way out of whack.

Continuing with our core server example, with baselining and standard deviations, the fill-in NOC staff member, without any familiarity with that server, can instantly contrast how it is behaving now with how it behaves normally, and draw some fast and accurate conclusions.

Another example of highly useful analytics capabilities is synced time series analysis. Users benefit from these views because they factor in elements of the organization's business logic. Perhaps it's a ticket agency with high activity before big games, or a check-cashing company with spikes of activity on paydays. These analytics can incorporate real-world factors such as holidays, busy periods, production schedules, maintenance windows and more. Without needing to know these details, NetOps with analytical capabilities such as these at their disposal can instantly see the patterns and use them in their decision-making processes. It's another way that a modern network monitoring system can significantly increase teams' network monitoring operational efficiency.

Step 3: Add context to highlight priorities
In modern networking, tools that network managers and engineers need to look at are well known, and at some level, fairly consistent from one network to the next. Because of the nature of network resources and the importance of activities they support, these aspects are naturally viewed by NetOps and engineering teams in the context of their importance to the business.

Modern network monitoring systems can factor in the importance of specific devices and other network resources and include prebuilt ways to quickly visualize them to provide users with instant context. Capitalizing on knowledge of the current network devices and data structures they use, modern monitoring systems provide intuitive ways for users to easily see and quickly understand what is happening in their network environments.

This context can come from the addition of elements such as user-defined color ranges, performance status icons, performance limits or boundary lines. To help users make the most of this context and quickly go from awareness to understanding to action, single-click drill-downs into device, object or indicator specifics are a key feature, as are easy ways for users to link visualizations to reports.

Again, without intimate knowledge of a particular set of devices and their usual behaviors, a NetOps or IT pro can simply glance at one of these visualizations and immediately gain valuable context about a network issue. Giving teams the ability to quickly see and prioritize issues that need the most attention is another way that modern monitoring solutions enhance teams' operational efficiency.

Step 4: Build reusable visualizations and reports
A stubborn challenge for network teams is monitoring their environments efficiently across organizational silos and technological boundaries. Modern network monitoring solutions help teams get over those hurdles by enabling consistent and unified reporting across multiple sites and separate operational groups, and by enabling the rapid generation of highly scalable reports.

Fueled by all the collected data with analytics, and presenting it through compelling and intuitive visualizations, next-gen monitoring systems enable the creation of customized and reusable (time-saving) reports and visualizations. Examples include custom tables along with sankey, pie, bar, line, gauge and trending visualizations.

The best monitoring systems do more than just give users better ways to gather and analyze performance data. They also provide users with smarter, faster and easier ways to shape their performance insights and share them across their organizations. By bringing insights to life in timely, actionable and visually compelling reports, modern monitoring solutions let networking teamstake their own performance to the next level.

Step 5: Create problem-solving automation workflows
Network observability systems deliver the most value when they arm teams with the performance intelligence they need to locate, diagnose and resolve network problems quickly—or better yet, prevent issues from becoming problems. That's where customizable, reusable and shareable automation workflows that turn insights into actions make all the difference.

Modern monitoring systems offer powerful, flexible tools for creating customized automation workflows. Whether you leverage sets of pre-built automation workflow templates or create your own via out-of-the-box, drag-and-drop, low-code building blocks across network and security infrastructure, applications, and more, your teams can seamlessly build additional workflows to automate tasks and processes tailored to their network requirements. An automation engine integrated as part of your network observability system enables NetOps professionals to facilitate network automation and simplify the integration of diverse network technologies without extensive coding knowledge.

Conclusion

To achieve their goals and minimize the service delivery risks associated with today's complex IT environments, organizations need to boost network monitoring operational efficiency. The first step is to put comprehensive, scalable and flexible data collection in place. Once organizations have this performance visibility, they can develop or strengthen the other required capabilities: using analytics, adding context, building visualizations and reports, and developing customized and shareable workflows.

To really "move the needle" and significantly increase their network monitoring operational efficiency enterprisewide, networking teams need solid performance insights. Those insights must be accurate, detailed and delivered quickly. They also have to be actionable and scalable. That means they must have utility and applicability for various teams, including operations, IT, engineering and line-of-business groups.

IBM SevOne

As organizations rearchitect their networks with newer technologies such as next-gen wifi, SD-WAN, SDN, multicloud, 5G and more, they need to make a parallel change with their network monitoring. New infrastructures require monitoring systems that are just as dynamic, flexible and scalable as the new environments are.

There's a reason why hundreds of top enterprises, CSPs and MSPs worldwide have chosen IBM SevOne as their network monitoring solution. The reason is that it delivers.

IBM SevOne provides application-centric, hybrid network observability that turns insights into actions to help NetOps spot, address, and prevent network performance issues. Boost network performance and improve user application experience by proactively monitoring and automating multivendor end-to-end networks across enterprise, communication, and managed service provider environments.

By transforming raw network performance data from infrastructure using machine learning across the entire delivery chain into actionable insights, and then through an integrated low-code, no-code automation engine that turns insights into actions, IBM SevOne delivers a comprehensive view of what's happening in the hybrid cloud network and how that performance affects the applications driving modern businesses. IBM SevOne can automate tool integrations and network actions based on ML observations, reduce repetitive tasks, and ensure coverage and compliance. The solution is designed to meet the agility, reliability and business efficiency needs of modernized organizations with application-centric insights and automation to optimize a modern network.

The fact is, to actually gain all the benefits of a modern, digital infrastructure, organizations need a monitoring solution that has no trouble keeping up. That solution is IBM SevOne.

Learn more about IBM SevOne.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2024

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.