Enterprise network operators today have an unprecedented amount of network health and performance data. But harnessing that data for maximum benefit is an immense challenge and requires a modern cloud-supported, machine learning–powered analytics platform.

Network Visibility and Analytics: Gain Insights and Actionable Data from Your Network

December 2019

Written by: Brandon Butler, Senior Research Analyst, Enterprise Networks

The Importance of Network Visibility and Analytics

The enterprise network has never been a more critical enabler of technology innovation. It provides essential connectivity for the most important new technologies, IT systems, and business applications that businesses rely on. The advent and mainstream adoption of cloud computing, big data analytics, and mobile-first network architectures have enabled great opportunity. But these 3rd Platform technologies, as IDC calls them, have also placed tremendous strain on the network and are causing operations teams to struggle with how to ensure the network is able to meet the needs of the business.

In response, enterprises are demanding greater levels of insight into what is happening in their networks. This critical information is used for a variety of tasks. At a basic level, understanding what is happening within the network is the first step toward ensuring it is performing the way that it should be. At a more advanced level, visibility and analytics insights can be used as foundational information for automating and securing enterprise networks. Enterprise networking professionals can't protect, or automate, what they can't see.

Recent Advancements in Visibility and Analytics

While enterprises are developing a greater understanding of the value of network analytics data, it is becoming more difficult to collect the deep levels of pertinent visibility and actionable insights that tangibly improve operations. There are a variety of reasons for this. First, the traditional definition of an enterprise network has evolved. Organizations are no longer managing the various aspects of their networks in silos, even though it can be relatively easy to gain point-in-time visibility into siloed environments. Enterprises are increasingly integrating their management of wired and wireless LANs, plus branch offices and connectivity to Internet of Things (IoT) devices. But previous-generation visibility tools have been designed to work in previous-generation siloed environments, customized to providing a view into a specific area of the network.
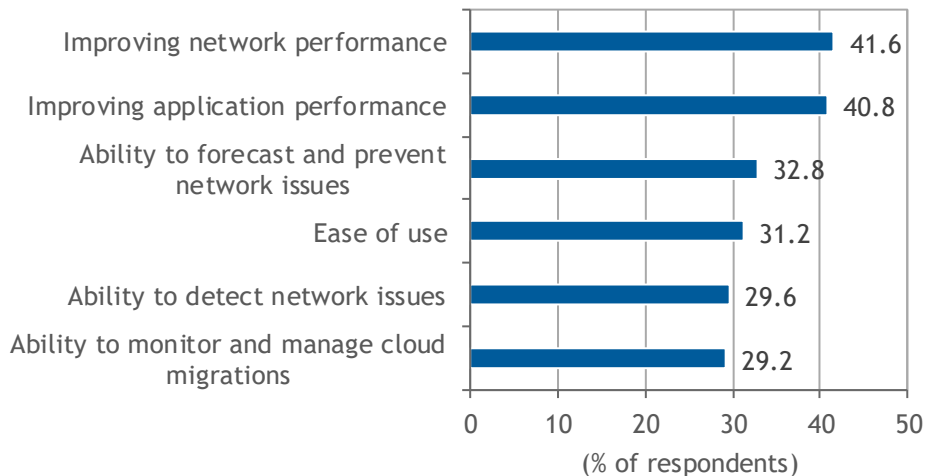
AT A GLANCE

KEY TAKEAWAY

As networks have grown not only in importance but also in complexity, getting detailed visibility and analytics of network operations becomes critical for ensuring the network is performing optimally and securely.

Meanwhile, the capabilities available to monitor and analyze network operations have increased significantly in recent years. Enterprise networks produce substantial amounts of data: Every connection on the network creates a series of data and metadata. This data can be mined, collected, aggregated, and analyzed.

To do so, however, requires a platform approach: Without a system to collect and analyze this data, it is merely a firehose of information. Modern visibility and analytics platforms have been developed that centrally collect, categorize, and analyze network-specific data. Typically, they have a graphic interface with intuitive controls, allowing network operators to customize views at an enterprisewide high level, or the ability to drill down to individual connections and network components. Figure 1 shows the top factors that enterprises are looking for from their performance management systems.

FIGURE 1: *Top Factors Driving Performance Management System Selection*

Q *What were the three most important factors driving the selection of your performance management systems?*

Factor	% of respondents
Improving network performance	41.6
Improving application performance	40.8
Ability to forecast and prevent network issues	32.8
Ease of use	31.2
Ability to detect network issues	29.6
Ability to monitor and manage cloud migrations	29.2

n = 250

*Source: IDC's NPM Study, December 2017*

The cloud is another major advancement that has led to a resurgence in network visibility and analytics data. The cloud is a central platform where data from disparate parts of the network can be aggregated. Once data is aggregated in the cloud, advanced analytics platforms can crunch the data that powers the customer dashboards.

How Machine Learning and Artificial Intelligence Impact Visibility and Analytics

Perhaps one of the most important trends impacting network visibility and analytics has been the advent of machine learning (ML) algorithms. ML algorithms feed off data — the more data they have, the better they are. This makes network analytics an ideal use case for applying ML technology to help optimize operations and provide actionable intelligence. Figure 2 shows the strong promise that enterprise IT professionals see in using ML and artificial intelligence (AI)-enabled technologies in network operations.

FIGURE 2: *Top Priorities for AI-Enabled Network Automation*

Q *What do you see as the most important aspects of AI-enabled network automation?*
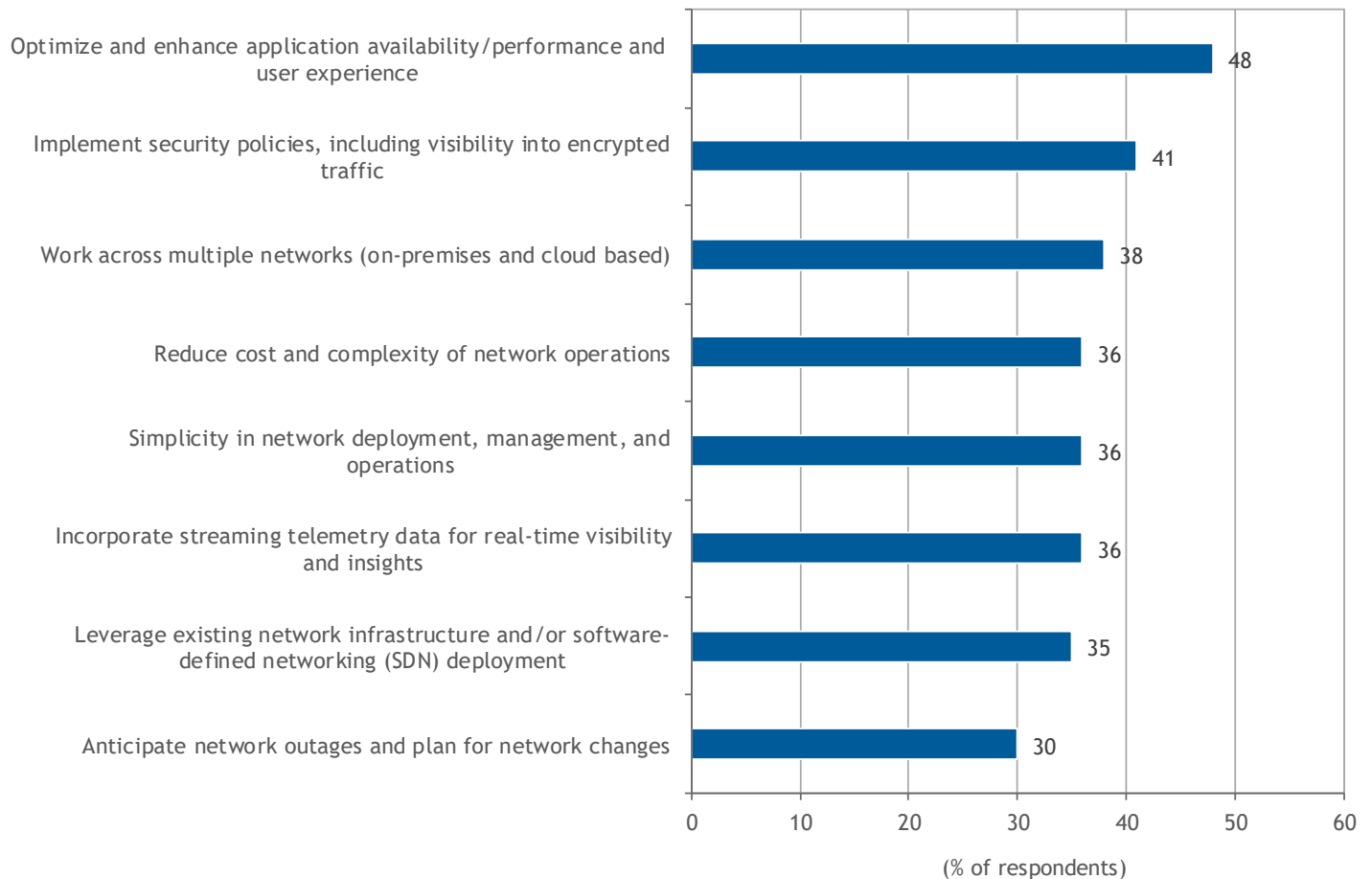
n = 301

Source: IDC's IT Strategy and AI Adoption Survey, February 2019

One of the strengths of ML algorithms is recognizing anomalies in data. If an ML platform monitors an environment, it learns what "normal" behavior is and, even more important, what abnormal behavior is. Anomalies usually represent a problem, either in security or performance degradation. The ML-powered system can create an alert based on the anomaly, notifying network operators of the issue and even recommending a way to fix it. In the future, these systems will advance to become artificially intelligent. AI-driven systems take automatic actions to maintain the optimal operating environment based on ML insights. The following would be an ML- and AI-powered network analytics and operations workflow:

» Visibility platform collects data across the entire enterprise network and correlates it to a central repository.

» ML-powered platforms detect an anomaly, signaling a security or performance degradation.

» ML platform identifies the root cause of the problem based on its learnings of network operations.

» ML platform provides a recommendation of how network operator can fix issues.

» AI-based platform automatically implements high-confidence, low-impact fixes.

» Network operators can conduct additional tasks on the AI system as they become more comfortable with it.

Eventually, the network becomes self-driving, meaning network operators dictate the desired state of the environment and an AI-powered platform dynamically implements and maintains that state, even as conditions on the network change.

Considering Ruckus Analytics

Ruckus Analytics from CommScope is a new cloud-based platform for providing deep levels of visibility and customizable analytics for network operators. The platform can be set up to automatically collect data from central points in the network and aggregate telemetry related to health data and key performance indicators (KPIs) across the enterprise network. Anonymized metadata is sent to a cloud-based analytics engine that serves as a data lake for queries, reports, and metrics.

Ruckus Analytics collects data across dozens of dimensions, including time, device type, traffic type, application, access point (AP) group, controller, and service set identifier (SSID). Users interface with this information through a drag-and-drop graphical user interface (GUI) that provides auto-ranked visibility into the most important problems in the network. Customizable dashboards allow users to drill down into data at the per-client or per-device level. The platform helps optimize operations across multiple areas of network management, including:

» Network traffic and client trends, including top SSIDs

» Client makeup of the network by operating system (OS), device manufacturer, top client usage, client trends, and session details

» Inventory — existing deployment information by AP, switch, and controller counts; models; and firmware status

» Applications — top applications, usage trends, top parts

Data is available in pivot tables, line charts, bar charts, and heat maps and is downloadable as raw data or in PDF or CSV format.

Challenges

Despite the advanced capabilities that recent network analytics platforms have developed, not all organizations have realized the true potential these technologies can enable. Too often enterprises are busy "keeping the lights on" and have not thought about ways that advanced technologies, such as analytics platforms, can help improve operations. This will be a challenge for vendors such as CommScope as they look to show the tangible benefits these systems provide.

Another challenge will be the variety of purpose-built network performance management (NPM) platforms on the market that offer a wide range of visibility and monitoring functions. The Ruckus Analytics platform, however, is ideally suited to provide deep levels of insights into Ruckus environments.

Conclusion

The network is at the heart of every enterprise's connectivity to customers, internal stakeholders, and the broader world. That's why it is so important to ensure the network is secure and performing optimally. The best way to get these insights is to have a system that is powerful enough to automatically collect, correlate, and analyze that network data. Recent advancements in platforms built for these purposes have made them powerful tools for network operators. Enterprises now have greater access than ever before to granular levels of insights, and much of this information is based upon machine learning.

The benefits of analytics-based network data are multifold: The information allows organizations to understand exactly what is happening in their networks at any time, both at a high level across the entire network and down into the individual components. It will also help organizations automate tasks, recognize security incidents or performance degradations, and resolve the incidents or degradations before they impact users.

About the Analyst

Brandon Butler, *Senior Research Analyst, Enterprise Networks*

Brandon Butler is a Senior Research Analyst with IDC's Network Infrastructure group covering Enterprise Networks. In this role, he is responsible for market and technology trends, forecasts, and competitive analysis in Ethernet switching, routing, wireless LAN, and adjacent emerging segments such as SDN and SD-WAN.

MESSAGE FROM THE SPONSOR

About Ruckus Analytics and CommScope

Ruckus Analytics from CommScope is cloud-based software that provides detailed reporting, informative dashboards and machine-learning-powered analytics for Ruckus networks. CommScope added the Ruckus product line to its portfolio when it acquired ARRIS in April 2019.

CommScope (NASDAQ: COMM) helps design, build and manage wired and wireless networks around the world. As a communications infrastructure leader, we shape the always-on networks of tomorrow. For more than 40 years, our global team of greater than 20,000 employees, innovators and technologists has empowered customers in all regions of the world to anticipate what's next and push the boundaries of what's possible. Discover more at *www.commscope.com*.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com**.**