12TH ANNUAL

STATE OF THE NETWORK STUDY

VIAVI Solutions

STATE OF THE NETWORK

EXECUTIVE SUMMARY

The 12th annual Global State of the Network Study captured the insights of more than 600 NetOps and SecOps professionals, highlighting their challenges in security, performance management, and deployment of new technologies with an emphasis on today's threats to IT.

This year's study revealed the escalating demands faced by NetOps teams as they are pulled into security efforts at a growing rate. This continually increasing focus on security creates "mission creep" for NetOps teams that could compromise their ability to maintain network performance and troubleshoot user issues.

Key findings from the 2019 State of the Network Study include:

- Network teams are critical to protecting business resources and strengthening IT security initiatives. Significant increases in threat workloads were reported, with nearly 90 percent stating they spend up to 10 hours or more per week—these same respondents indicated this is up 25 percent in the past 12 months.
- NetOps teams are now playing an active role in aiding SecOps organizations before, during, and after a threat has been detected due to the increase in volume and sophistication of security threats.
- Respondents highlight the importance of understanding normal network behavior and the ability to quickly hunt for malefactors when suspicious activity is noted.
- Wire data has now taken a central role when resolving suspected or known security incidents.
- There is an acceleration of collaboration between SecOps and NetOps teams to maximize security initiatives before incidents occur and minimize clean-up time after breaches have been confirmed to limit negative impact to the business and customers.
- While NetOps teams pivot to assist with security, they are still challenged to maintain acceptable service performance and end-user experience despite the rapid deployments of new technologies and large increases in network traffic loads.

STATE OF THE NETWORK

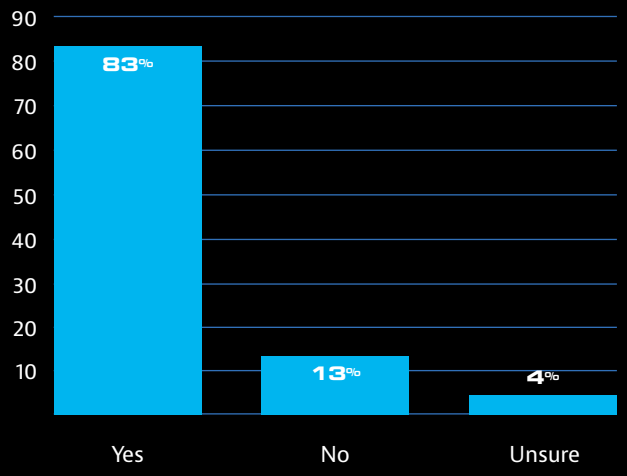
HEAVY SECURITY WORKLOADS

The ongoing convergence of NetOps and SecOps duties continues to increase. Security issue resolution is now front and center for more than 4 in 5 network teams.

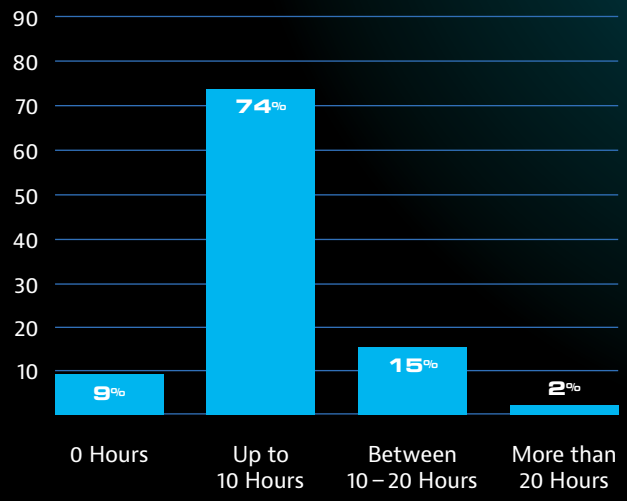
As the threats grow, workloads to address them also continue to expand. 83 percent of Network teams are involved in resolving security issues.

74 percent stated they spend up to 10 hours per week with another 17 percent specifying significantly more.

Is your organization's network team involved in resolving security issues?



What percent of a 40-hour work week do you spend resolving security-related issues?

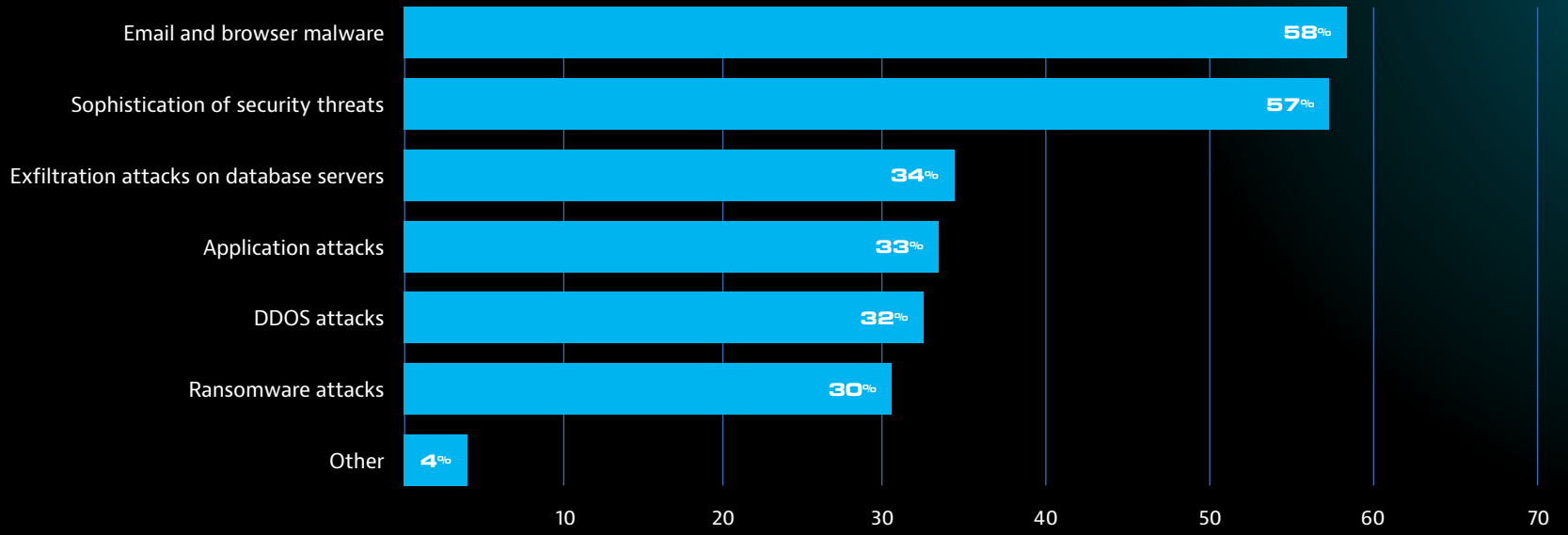


KEY TAKEAWAY: **Network teams are now, more than ever, involved in maintaining IT resource integrity and their time commitment in assisting the security groups continues to grow. Given this, it's important that senior management account for their central role as protector of critical business resources through proper staffing and financial support.**

ESCALATING ATTACKS

Email and browser malware are cited as the fastest growing threats in the past 12 months with nearly 60% of respondents calling them out. Meanwhile, numerous other threat vectors also experienced material growth.

Have the following network security threats increased in your organization in the past 12 months?

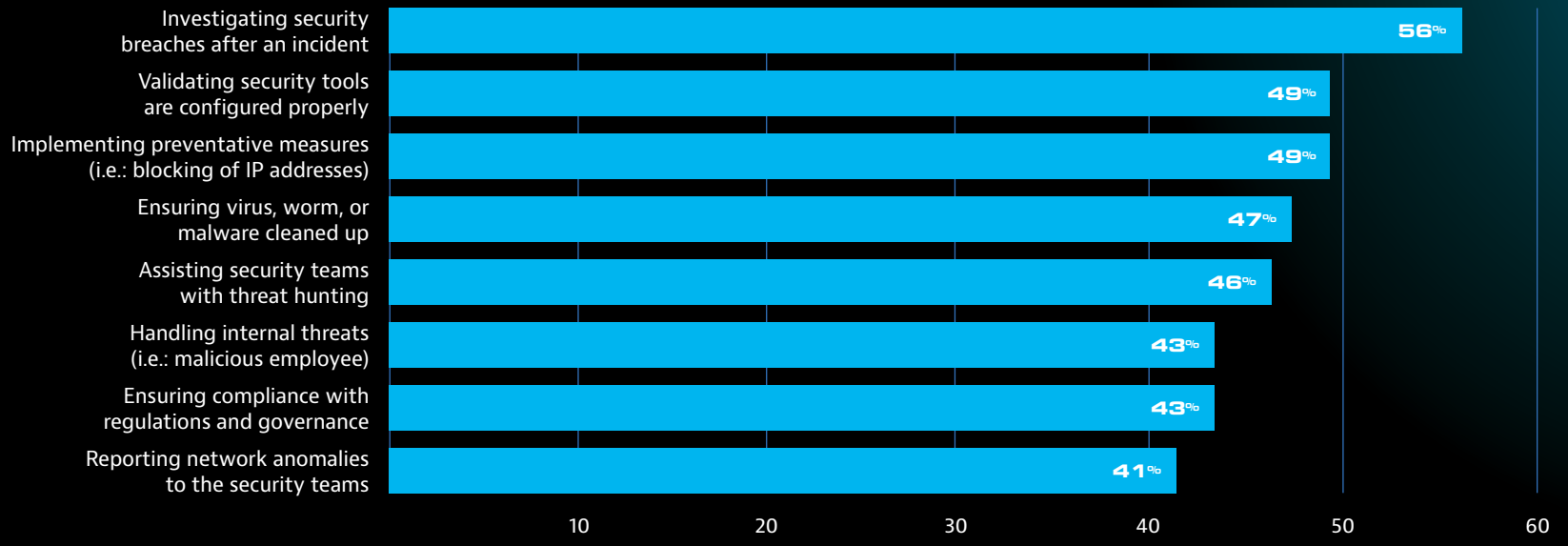


KEY TAKEAWAY: **There's no let-up in sight for NetOps and SecOps teams as they continue an endless battle with hackers seeking to breach existing security perimeters. Those responsible to protect must remain vigilant and constantly assess their strategies, updating and reinforcing as required to meet the challenge.**

NETOPS TO THE RESCUE!

More than half of network teams indicated their top security role is in the forensic investigation after a breach has been detected. Other important duties include validation of security tool configurations—the second most common response in the survey—while assisting in implementing preventative measures, fills out the number three spot at nearly 50 percent.

What role does your network team have in handling security?



KEY TAKEAWAY: **Though investigating breaches after the incident remains the number one role, network teams are moving well beyond that by aiding SecOps in multiple ways. Interestingly two of the eight roles are very proactive, the first being threat hunting which involves looking for aberrant behavior while the second, "Reporting network anomalies to the security teams" suggest they are finding potential threats before the security team is aware of them.**

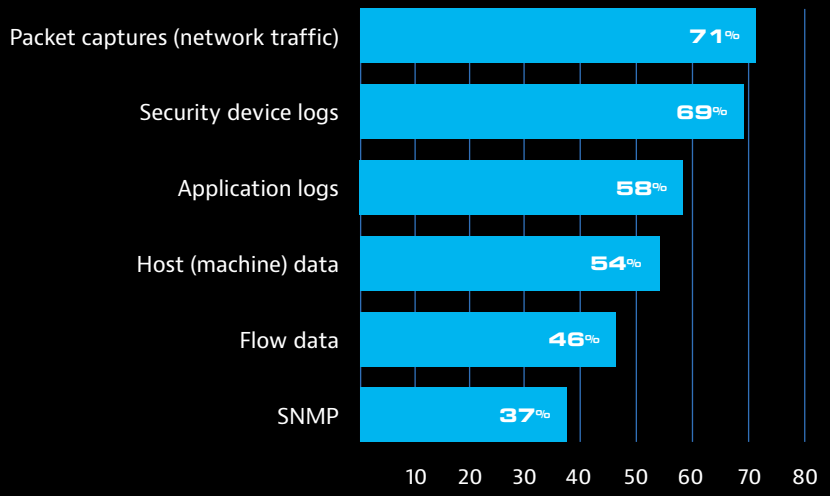
STATE OF THE NETWORK

WIRE DATA RETENTION

Network teams now depend on packet capture as their most important source of data for security incidents, a dramatic increase from the results of the 2017 State of the Network Study. A close second was syslogs whose value nearly equals network traffic information. Application logs, host machine, and flow data follow-up the list of most valuable sources.

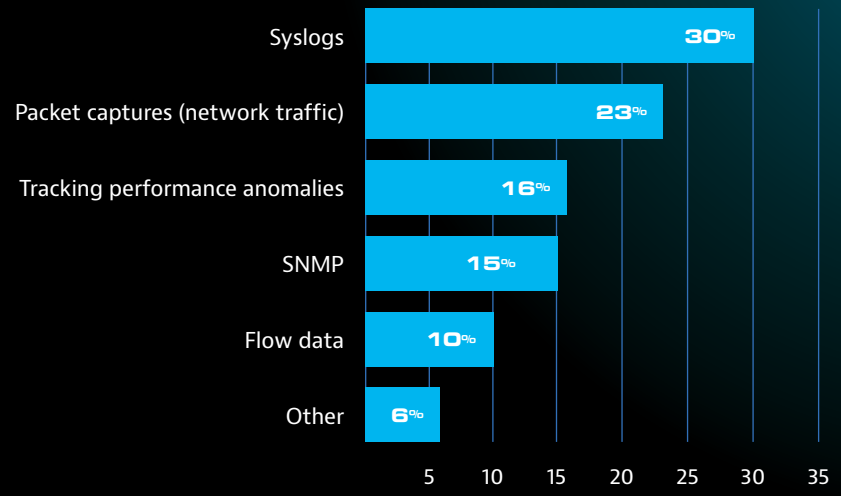
2019

What network data sources does your network team use for security incidents?



2017

What monitoring methods does your network team use for security incidents?

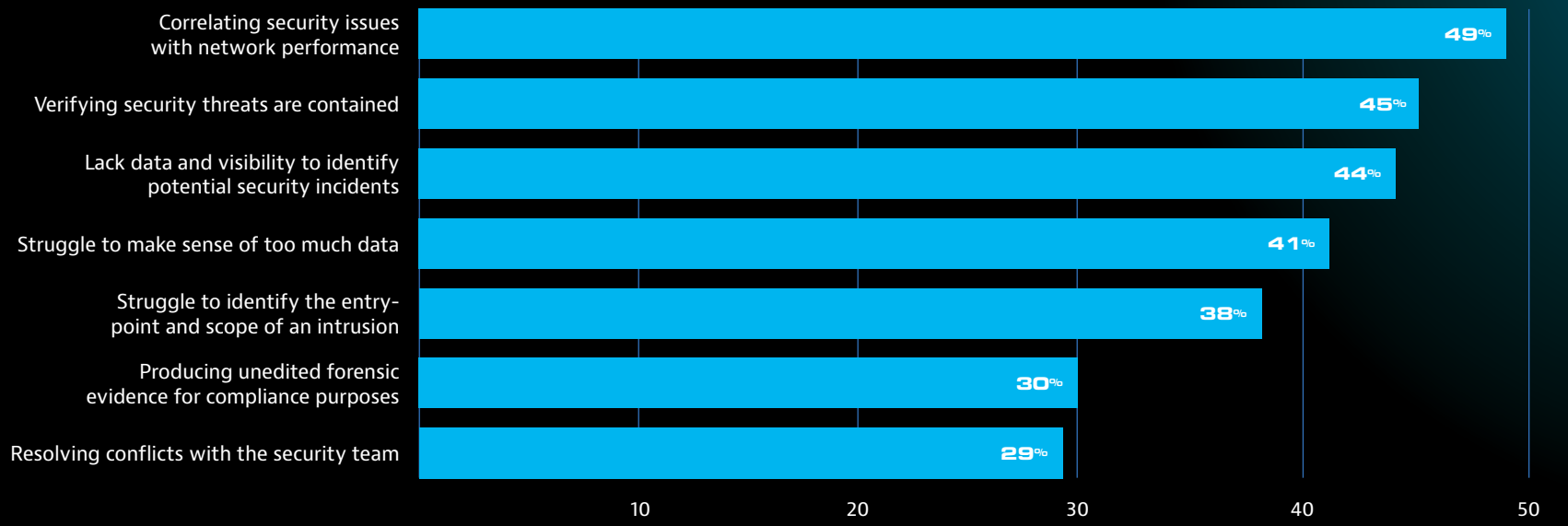


KEY TAKEAWAY: **The use of packet capture data nearly tripled in just two short years. As the maliciousness of malware grows and the negative exposure to business with it, having all the packets provides the ultimate peace-of-mind. With it, teams can ascertain exactly what transpired as suspicious conversations propagate across the network and which assets were potentially compromised. This complements the deep insight offered by syslogs at the individual device level and the other data sources.**

PROGRESS BUT NOT PERFECTION

As IT teams improve their efforts to better safeguard resources, the number, severity, and sophistication of threats grows in response. Most of the results speak to the bottom-line difficulties of detecting a threat that has circumvented existing security measures. Unless they are identified through unusual traffic volumes, questionable transaction patterns, or in the worst case, the divulging of sensitive information externally, security breaches often go undetected for extended periods increasing the potential corporate and stakeholder damage.

What are the largest challenges you face when addressing security issues?



KEY TAKEAWAY: **Given the high stakes for businesses if security threats are not identified and contained quickly, IT teams cannot depend solely on dedicated security tools to safeguard resources. Instead, they need to "know their network", understanding what is normal and what is not—looking for even the smallest anomalies as hackers adapt to subvert AI and machine-learning tools. Similarly, the need to perform "hunting expeditions" when suspicious behavior is noted is a must. Networking and security tools that facilitate these activities can greatly simplify these initiatives.**

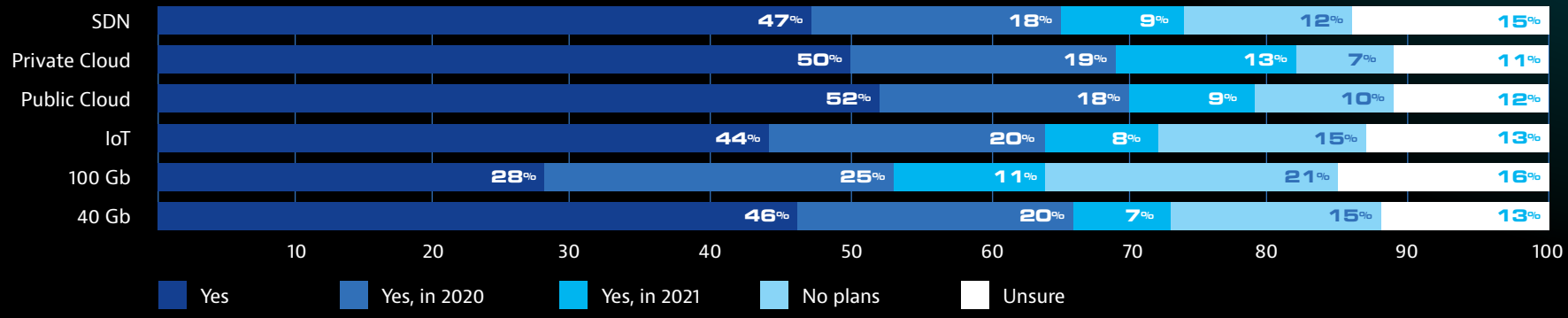
NEW TECHNOLOGY DEPLOYMENTS

Since its inception in 2008, the State of the Network Study has queried IT professionals on emerging or new technology rollouts within their enterprise organizations. For the first time, this year IoT was included and the implementation plan results were surprisingly aggressive—nearly 3 in 4 businesses have rollout plans within the next two years. It appears that organizations have determined the tremendous upside IoT offers more than offsets the potentially highly disruptive downside of adding additional devices to the environment—specifically as it relates to performance monitoring and security concerns.

Meanwhile the deployment of more mature technologies proceeds unabated from past year's findings. Faster networks speeds, whether 40 Gb or 100 Gb are already in place at 45 percent and 28 percent of respondents' environments, respectively today. Implementations plans suggest these numbers will grow to more than 70 percent and nearly 64 percent by 2021.

In terms of public and private cloud deployments, IT teams expect to reach around 80 percent for both by 2021 with the remaining unsure or having no plans to proceed with rollouts. Lastly, SDN results are roughly in line with last year's survey findings with approximately 3 in 4 planning to deploy by 2021.

Has your organization implemented, or will it implement the following network-related technologies?

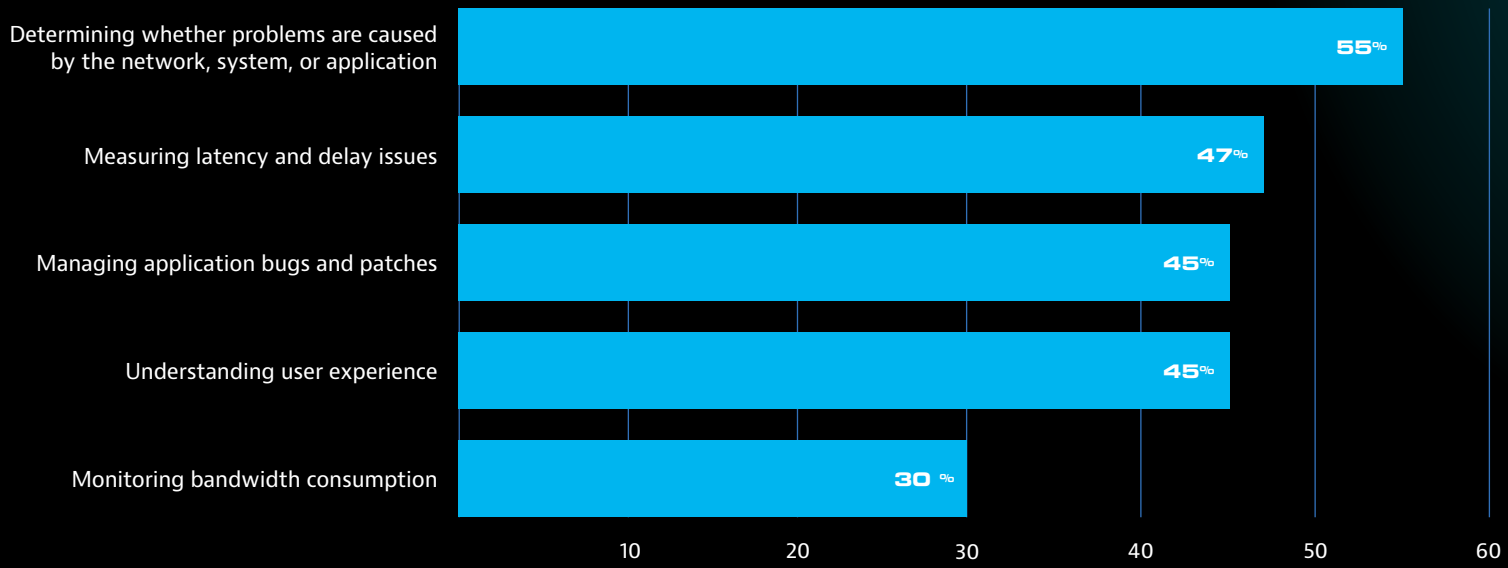


KEY TAKEAWAY: **Monitoring challenges continue to mount, and pressure will increase to maintain resource integrity as network speeds surge, assets migrate to the cloud, and the number of devices (tied to IoT) rapidly grows. NetOps and SecOps teams would be wise to take steps to maintain visibility sooner rather than later.**

PERFORMANCE MONITORING CHALLENGES REMAIN

Problem domain isolation continues to be the biggest obstacle to troubleshooting applications—this has been the top concern for many years of the State of the Network Study. Others run the gamut from quantifying network link attributes such as latency, delay, and bandwidth consumption to managing application bugs and patches. Understanding end-user experience was also called out by many respondents.

What are the most common challenges you face when troubleshooting applications?

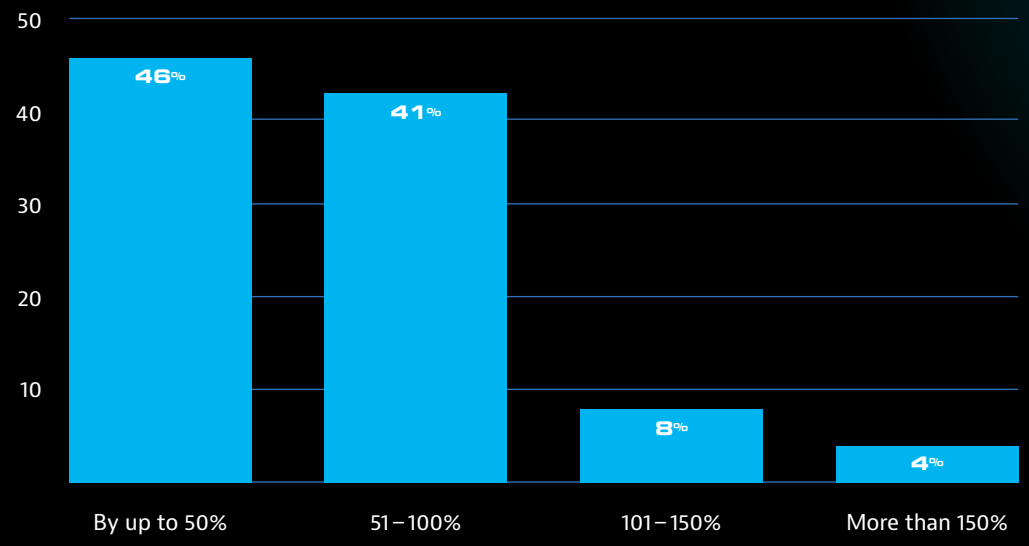


KEY TAKEAWAY: **The growing complexity of hybrid IT and service deployments, increasing device counts, escalating traffic loads, and network abstractions such as SDN are not lightening the troubleshooting loads or making service validation easier. Given this, NetOps teams would be best served by monitoring solutions that overcome these challenges to visibility while offering insight into problem isolation and end-user experience satisfaction.**

THE NEED FOR SPEED

Given the large number of existing and planned deployments of 40 Gb and 100 Gb networks, it shouldn't be too surprising that bandwidth demands are expected to likewise grow unrelentingly and that's exactly what this year's projections indicate. More than 4 in 10 expect up to 50 percent increase in bandwidth. Another 4 in 10 expect growth from 51 to 100 percent. Amazingly, roughly 10 percent are expecting more than 100 percent of growth in bandwidth.

How much do you expect the bandwidth demand for your organization's network to grow between now and 2021?



KEY TAKEAWAY: **IT teams should prepare for potential impacts to end-user experience as the amount of traffic rapidly multiplies.**

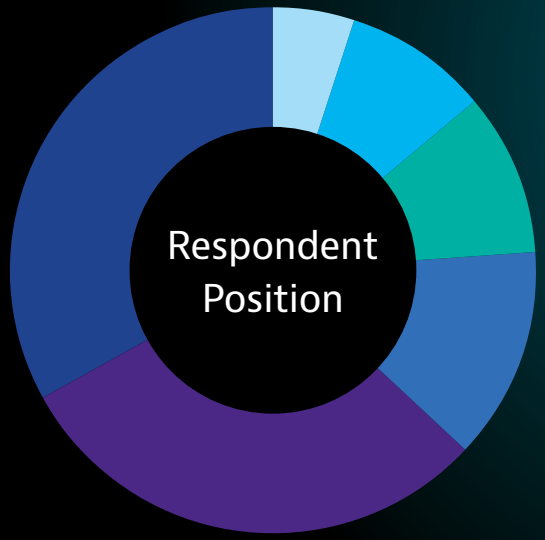
SURVEY METHODOLOGY

Study questions were designed based upon a survey of network and security professionals. Results were compiled from the insights of over 600 respondents from around the world.

In addition to geographic diversity, the study population was evenly distributed among networks and business verticals of different sizes.

Responses were collected in April of 2019 via online surveys.

For more information about the study's methodology or the results, contact Brad Reinboldt at brad.reinboldt@viavisolutions.com.



- 33% IT Manager/Director
- 30% Network Admin/Engineer
- 13% IT Consultant
- 10% CIO/VP of IT
- 9% System Admin/Engineer
- 5% Security Engineer

stateofthenetwork.com

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you,
visit viavisolutions.com/contacts

sotnreport19-wp-ec-ae
30190804 902 0719

viavisolutions.com