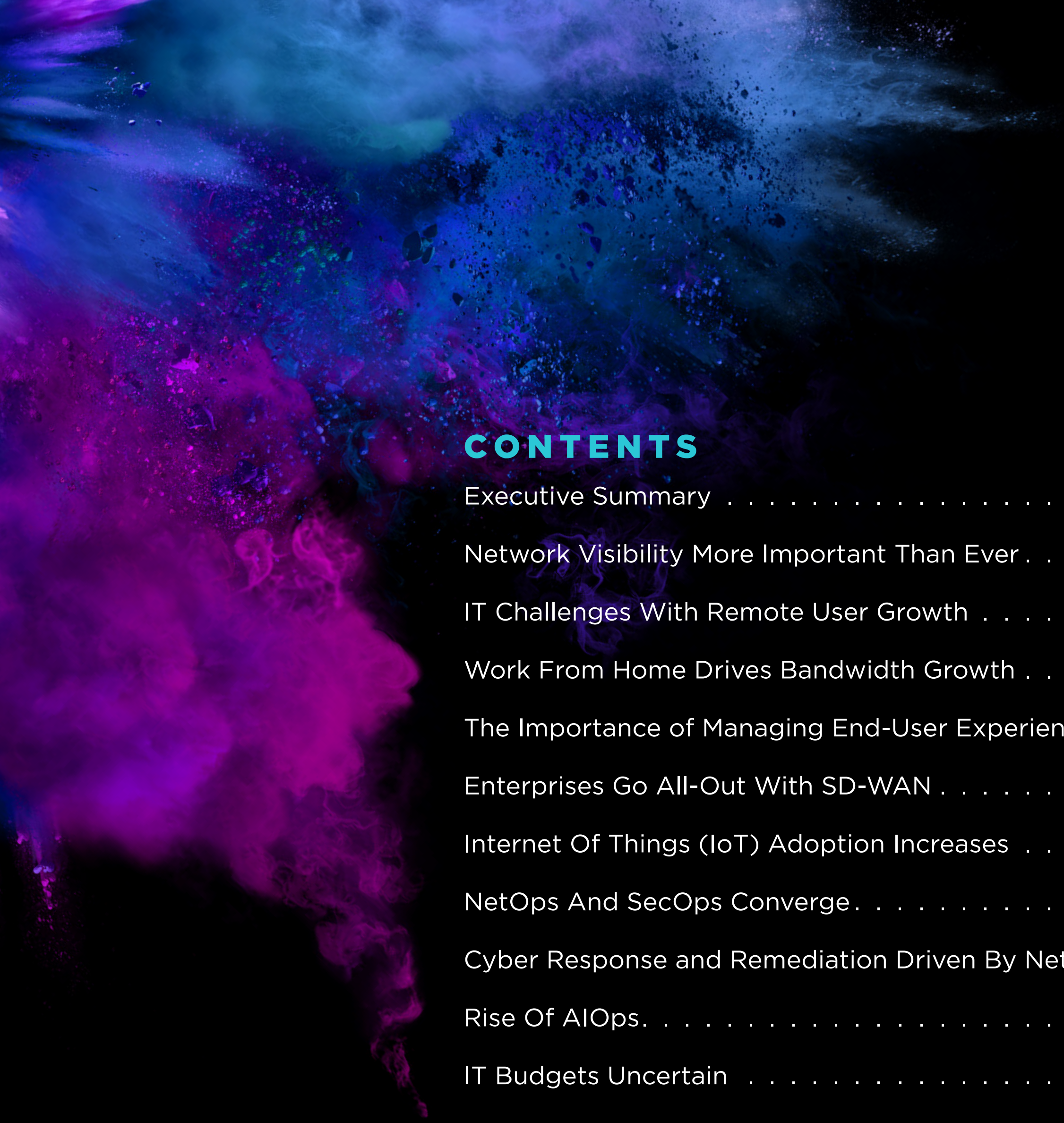
STATE OF THE NETWORK 2020

DISRUPTION

STATE OF THE NETWORK

VIAVI

VIAVI Solutions



CONTENTS

EXECUTIVE SUMMARY

The 2020 VIAVI State of the Network annual global survey of IT professionals demonstrates that IT is living in an age of dynamic disruption. In the midst of implementing remote working transition at an unprecedented scale and making emerging technologies go mainstream, NetOps and SecOps are increasingly challenged to maintain optimal service delivery.

How then can IT be enabled to overcome this turmoil? This survey suggests comprehensive network visibility as a crucial first step. It also highlights a growing awareness by all IT stakeholders of the underlying importance of a healthy network infrastructure to maintain peak service performance, reduce cybersecurity threats, and deploy new technologies.

The bottom line: empowering network, application and security teams means achieving ongoing operational excellence and moving beyond simply being a cost center to delivering business value to the entire organization.

KEY FINDINGS

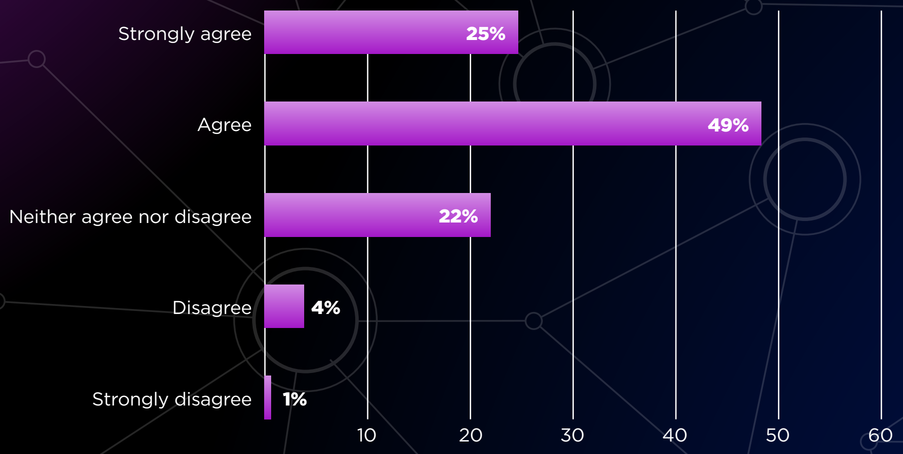
- For the first time in the thirteen years of the survey, **“understanding end-user experience” is the top challenge for troubleshooting applications** (nearly 47 percent) with the previous 12-year leader (“problem domain isolation”) falling to third place at 31 percent.
- **SD WAN has gone mainstream for organizations of all sizes**. Cost savings and business continuity being the primary motivations for deployment with more than 60 percent either having deployed, are deploying, or planning to deploy in the next 12 months but potential monitoring challenges lurk.
- **The rampant bandwidth growth in the previous year’s findings slowed slightly this year**, though 69 percent of respondents are still expecting up to 50 percent increases in traffic loads—independent of organizational size—**driven by remote users and cloud deployments**.
- **NetOps teams are feeling the pressure** with respondents stating more than 1/3 of their time (35 percent) is now consumed by efforts to resolve security issues, a dramatic jump from 2019 results; nearly 3 in 4 also agreed or strongly agreed that **SecOps need more visibility into the network**.
- **The surge in remote users is challenging network and security teams**—almost 58 percent are seeking more visibility—along with supporting resources (bandwidth load, maintain app performance, and VPN oversubscription)
- **The majority of businesses (64 percent) of all sizes leverage AIOps** calling out the benefits of “elimination of manual tasks” and “faster mean-time-to-resolution (MTTR)” but 4 in 10 have lingering questions about “data quality” and struggles with “skills gap”.

NETWORK VISIBILITY
MORE IMPORTANT THAN EVER

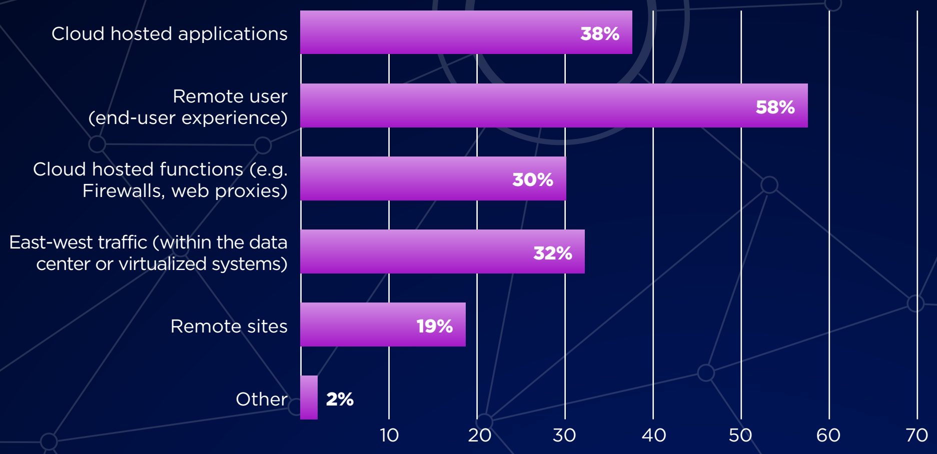
In 2020, visibility is king. SD-WAN deployment, application troubleshooting, security monitoring and remediation all rely on comprehensive network visibility to be most effective.

73% of respondents agree or strongly agree that SecOps teams need better visibility into the network to enhance the organization's cybersecurity efforts.

Our SecOps team needs better visibility into network and supporting infrastructure to enhance the organization's security posture.



What are the top 2 areas where you would like to have additional operational visibility?



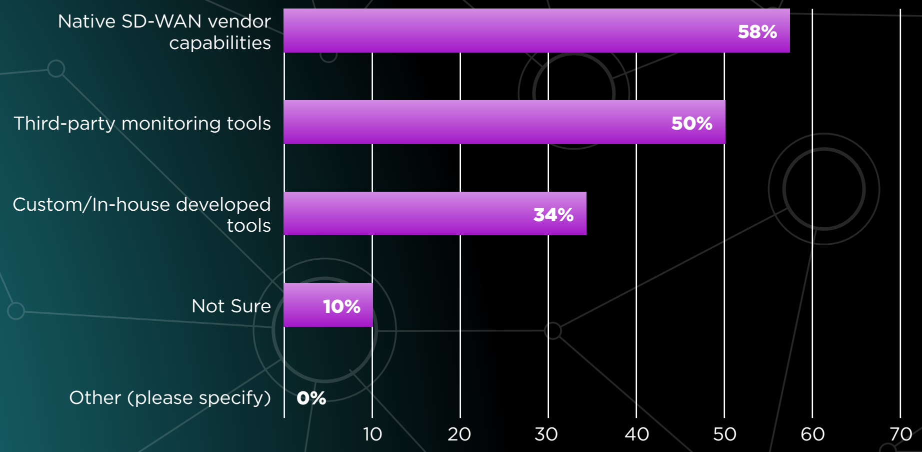
The recent surge in the number of remote users accessing corporate resources was reflected in responses here with nearly 58% calling it out, almost twice that of the next area of visibility.

NETWORK VISIBILITY
MORE IMPORTANT THAN EVER (CONT)

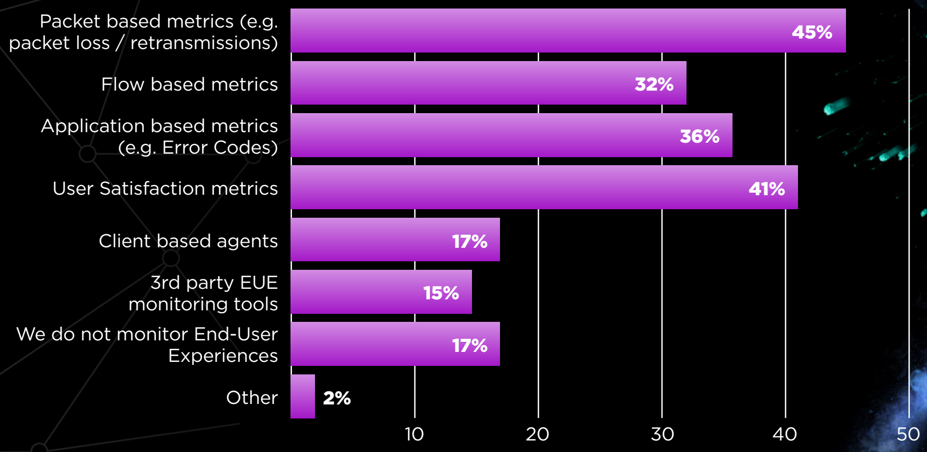
Most organizations plan to manage SD-WAN visibility by using only the vendor's native capabilities.

Packet-based metrics is the most used KPI for assessing end-user experience followed closely by user satisfaction metrics—this was true for organizations of all sizes.

How do you plan to manage SD-WAN visibility?



What metrics do you use to monitor End-User Experience (EUE)?



KEY TAKEAWAYS

When you have gaps in your network visibility, you have an incomplete picture. Network visibility is paramount to optimize critical processes including managing remote users, deploying new technologies , measuring end-user experience, detecting, and responding to security incidents, or troubleshooting application performance. Based on this year's results, packet-level data is the preferred method to accomplish this. In this age of disruption, senior stakeholders must recognize that network visibility drives IT operational excellence.

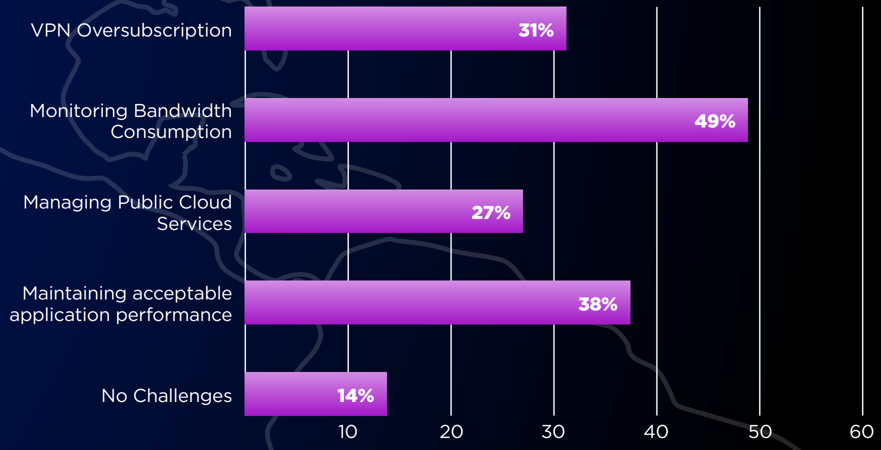
IT CHALLENGES WITH REMOTE USER GROWTH

The 2020 State of the Network survey shows IT teams grappling with disruption as they expanded their remote workforce at an unprecedented scale and compressed timeframe. Monitoring bandwidth consumption was the top management challenge during this transition, and lack of physical access to user device was the biggest service monitoring obstacle.

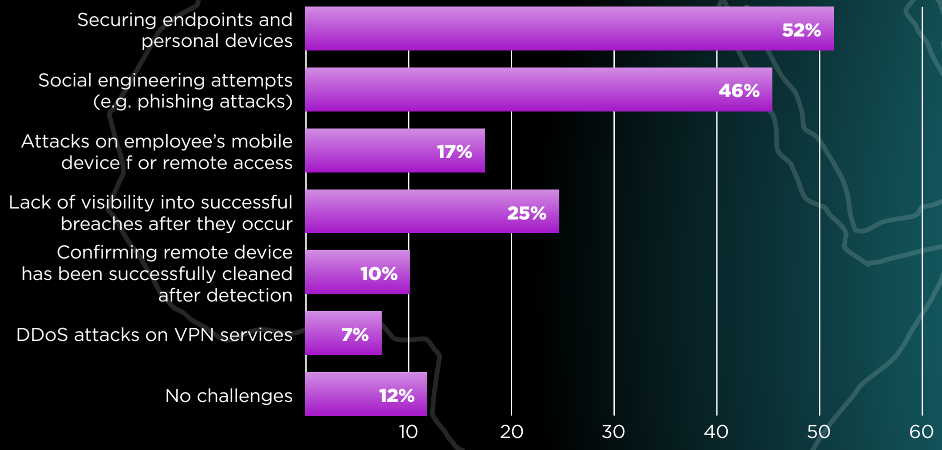
“Monitoring bandwidth consumption” was highlighted nearly 50 percent of the time, followed by “managing acceptable application performance” (37 percent) and “VPN over-subscription” (31 percent).

The inability to have physical access to the end user’s device was the top challenge in managing IT services, followed by interrupted performance of remote troubleshooting applications and decreased end-user experience visibility.

Since transitioning to a remote working environment, what are the top 2 network challenges you’re facing from managing remote user traffic growth?



What are your top 2 challenges in your IT team’s ability to manage services now that you are working remotely?



KEY TAKEAWAY

As increased remote working becomes the new normal for many organizations, IT teams are challenged to find effective management, monitoring, and troubleshooting strategies. VPN oversubscription, and troubleshooting applications. Network infrastructure that supports flow-based reporting can be a great resource here, providing volumetric information and additional application level insight. IT teams should use all native monitoring and management capabilities that are included by their VPN vendor. Combined, these increase visibility into remote user IT service health.

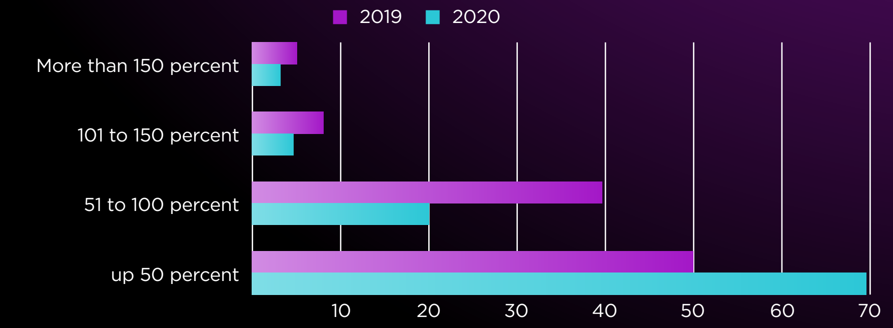
WORK FROM HOME DRIVES BANDWIDTH GROWTH

There was a moderate decline in year-over-year bandwidth growth across all organizational sizes, but bandwidth demand is still expected to grow due to increasing remote user access by "up to 50 percent".

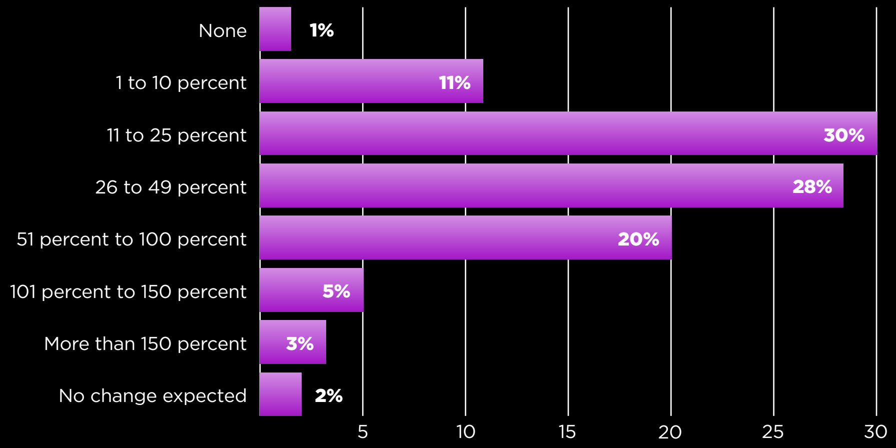
Interestingly, the data shows bandwidth growth was not distinguished by size of the organization with small and larger businesses reporting similar increases.

Remote user access and cloud hosting were the largest drivers of bandwidth growth across all business sizes with remote access clearly showing the largest and most rapid change, likely due to more users working from home.

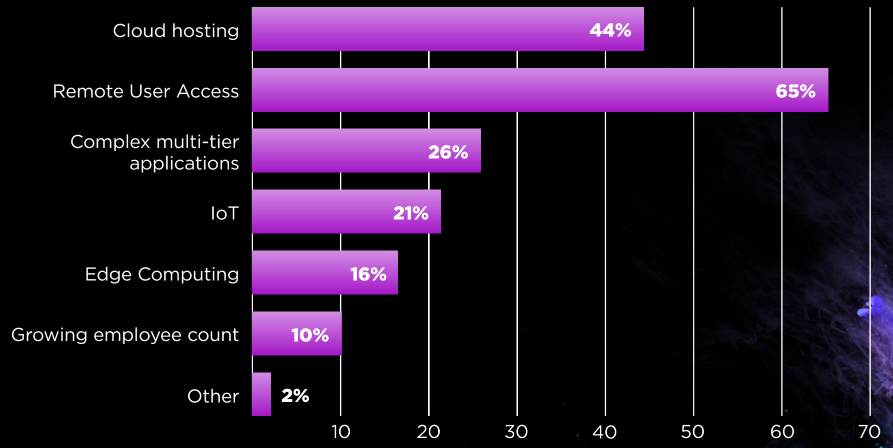
Bandwidth Growth 2019 vs 2020



How much do you expect the bandwidth demand to grow in the next two years?



What are the top 2 drivers of increasing bandwidth demand?



KEY TAKEAWAY

The growth of bandwidth consumption has been one of the constants with the survey since its inception—new technologies change, usage patterns fluctuate but the drumbeat for bigger network pipes is unrelenting.

THE IMPORTANCE OF MANAGING END-USER EXPERIENCE

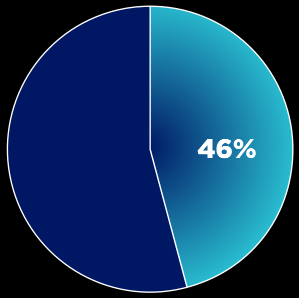
For the first time in the thirteen years of the survey, "understanding end-user experience" is the top challenge for troubleshooting applications (nearly 47 percent).

"Determining underlying network health (e.g. latency, retransmissions)" is the second biggest challenge when it comes to troubleshooting applications at 38 percent. "Problem domain isolation" falls from its 12-year leadership position to third place at 31 percent.

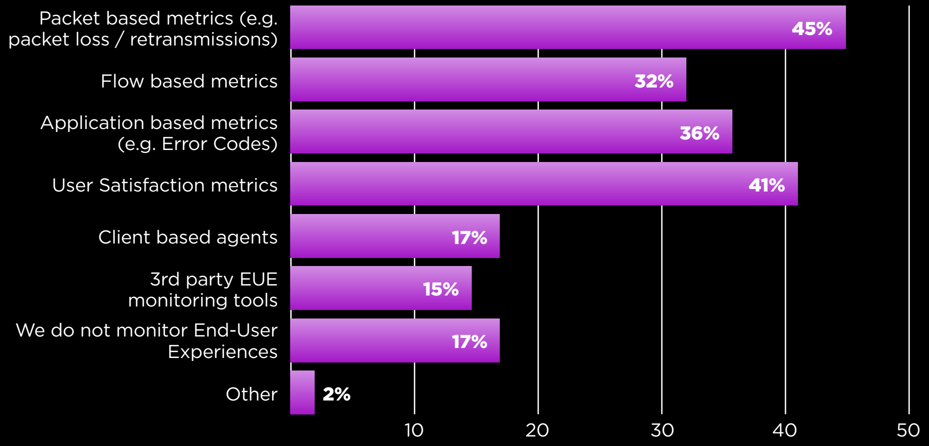
Even when broken out by company size, packets were the first or second most used end-user experience metric. Flow based metrics were the most common with mid-size organizations.

This year more than 45 percent of applications and services are now cloud hosted.

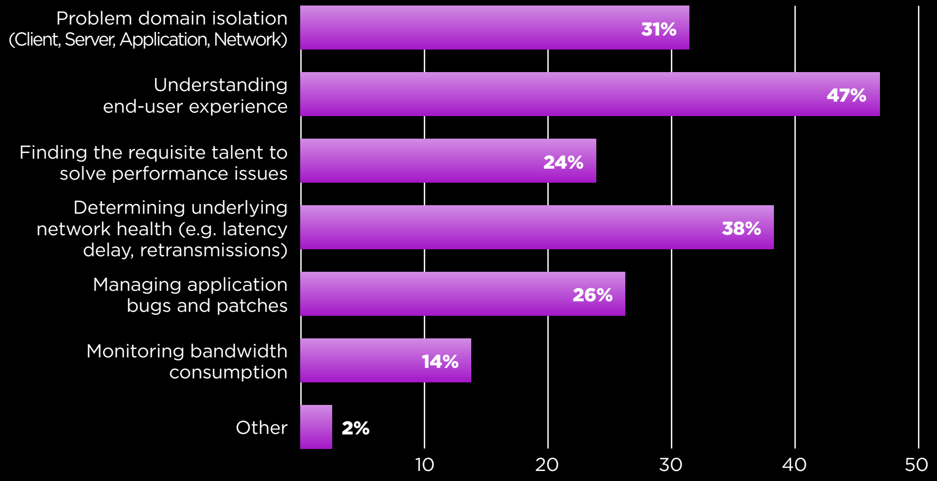
What percentage of your applications/services are now cloud hosted?



What metrics do you use to monitor End-User Experience (EUE)?



What are the top 2 challenges you face when troubleshooting applications?



KEY TAKEAWAY

IT Teams are beginning to acknowledge that end-user experience is the ultimate arbitrator of how well services are being delivered, and that the network can provide key insights to optimize service delivery. Given that IT teams need packet and flow-based data to fully understand the end-user experience, it's critical that an organization have the means to retrieve these insights for network performance and application troubleshooting. Finally, as more applications move to the cloud, IT management should consider ways to maintain adequate visibility into these services.

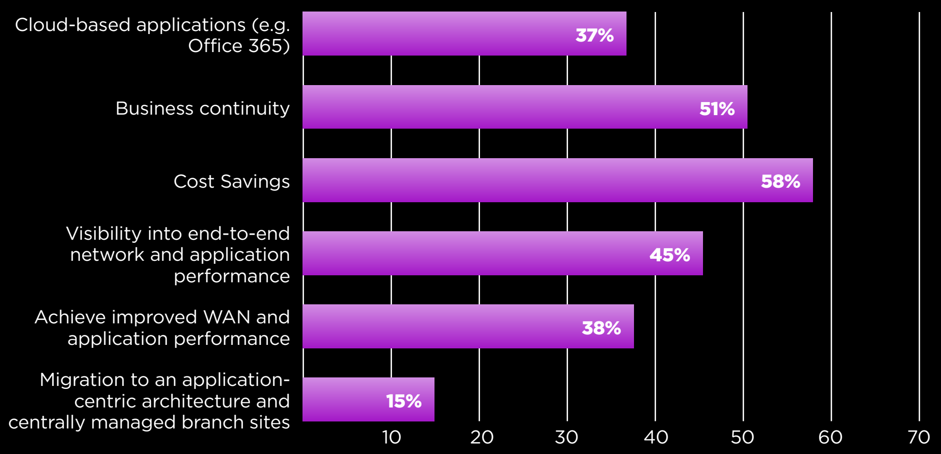
ENTERPRISES GO ALL-OUT WITH SD-WAN

Software Defined Wide Area Networks (SD-WANs) are becoming widely adopted, with more than 60% deployed, in process of deploying, or planned in the next 12 months.

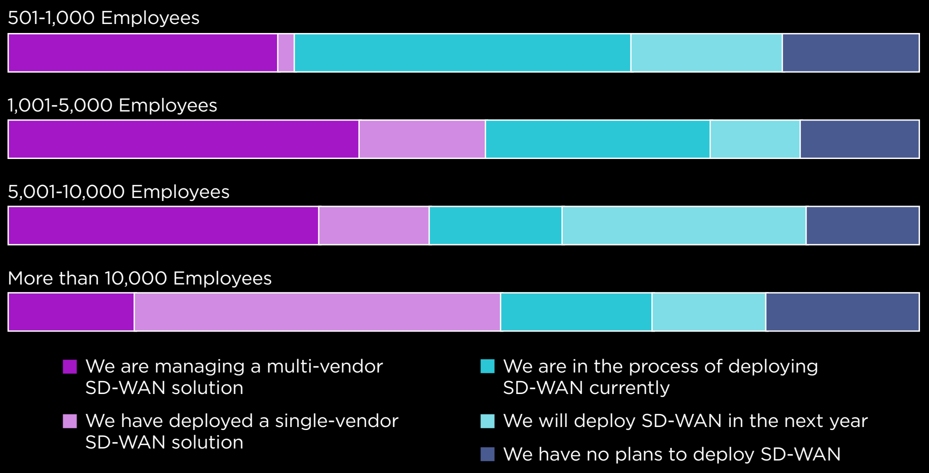
“Cost Savings”, “Business Continuity”, and “Visibility into end-to-end network and application performance” were the top drivers for deploying SD-WAN. For larger enterprises, “Visibility into end-to-end network and application performance” are the biggest motivators.

For medium to large businesses SD-WAN adoption jumps to 85%. Also, more than half of those that have or plan to have SD WANs in place use multiple vendors to do so.

What were your top 3 motivations for deploying SD-WAN?



What is the state of SD-WAN adoption within your organization?



KEY TAKEAWAY

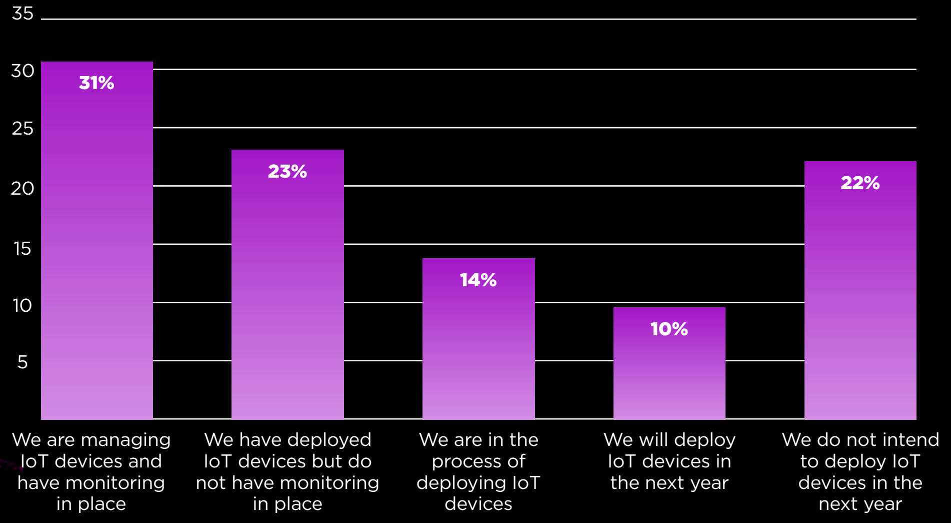
SD-WAN deployment has gone mainstream especially in larger organizations. Given that the majority use multiple vendors, it’s important that senior management recognizes how to integrate this technology. The goal of operational efficiency may be negatively impacted without the means to cross-check claims from SD-WAN vendors. To ensure business continuity and that cost savings are achieved with SD-WANs, comprehensive visibility into the network is critical.

INTERNET OF THINGS (IOT) ADOPTION INCREASES

More than half of survey respondents have already deployed IoT devices, up from 43 percent over last year.

Of those who have deployed IoT devices, nearly half have no mechanism to monitor those devices.

Describe the state of Internet of Things (IoT) deployment and device monitoring for your organization?



KEY TAKEAWAYS

As more IoT devices are added to the network, exposure to vulnerabilities and exploits are likely to escalate. Organizations are still coming to terms with how to integrate these new devices into their performance and security monitoring schema to achieve the operational efficiency with IoT without degrading security resilience. Given these observations, IT teams should begin at least strategizing how to monitor IoT devices sooner rather than later.

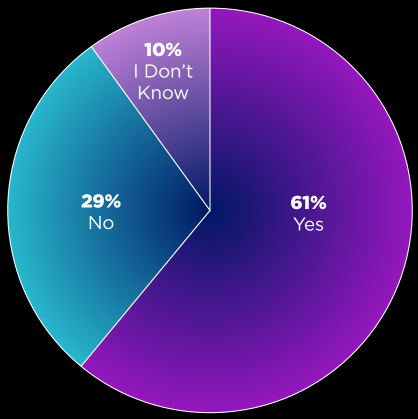
NETOPS AND SECOPS CONVERGE

Like in 2019, network teams are collaborating with security teams more than ever as the IT organization strives to maintain service uptime and strengthen cybersecurity initiatives.

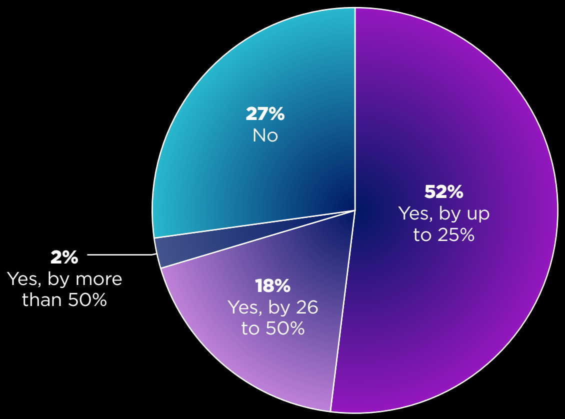
61% said that their network team was routinely involved in threat mitigation or investigations.

Regardless of employee size or industry, the amount of time spent resolving security issues for a given work week has grown significantly, from "up to 25 percent" last year to more than 35 percent.

Is your organization's network team routinely involved in threat mitigation or investigations?



Has the time you spend resolving security issues increased over the past 12 months?



KEY TAKEAWAYS

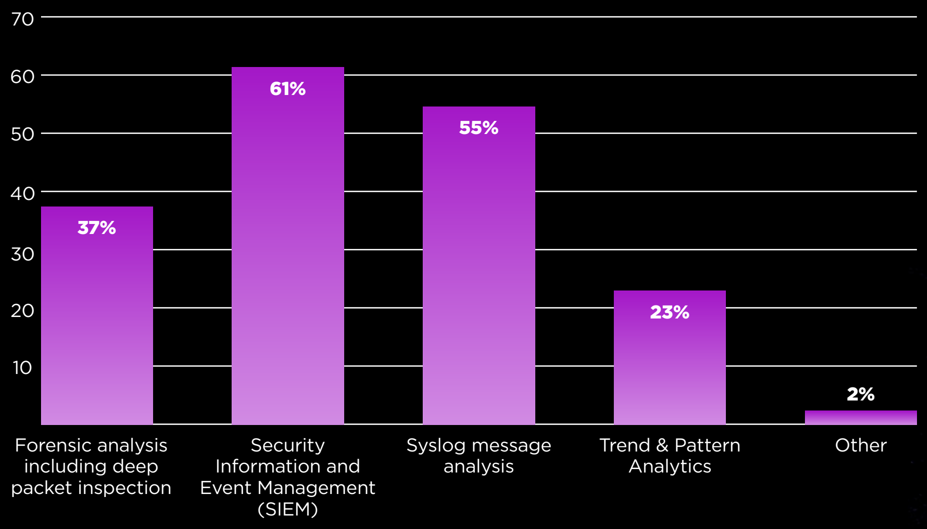
There is no letup in the need for NetOps teams to provide critical network visibility and to work closely with SecOps to achieve strong IT security and fast remediation when a breach inevitably occurs. This shift of time for the network team to security may impact their ability to address their typical duties such as maintaining optimal service delivery. More effective collaboration between teams is crucial to ensure all operational goals are achieved.

CYBER RESPONSE AND REMEDIATION DRIVEN BY NETWORK VISIBILITY

The SOC knows visibility into the network is critical to cybersecurity efforts. When it comes to post-breach remediation, security teams often make use of the forensic analysis of packets.

This is reflected in the results, with forensic analysis of packets being the third most important source of information behind only the traditional leaders of SIEM and syslogs.

What are the top 2 post-event breach remediation (clean-up) methods?



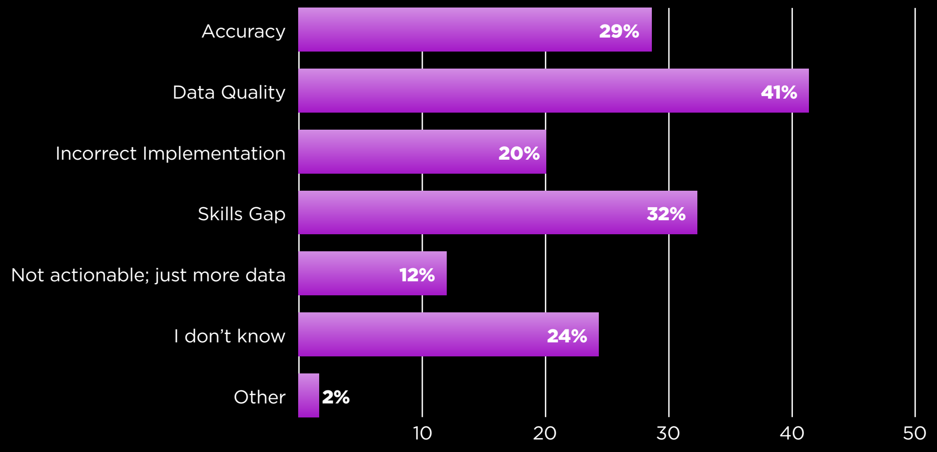
KEY TAKEAWAY

In addition to traditional SIEM and syslog, efficient remediation demands readily available forensic-level data to the security team. To maximize IT spend and foster tool consolidation, senior management must prioritize budget spend on solutions that can be leveraged by both NetOps and SecOps.

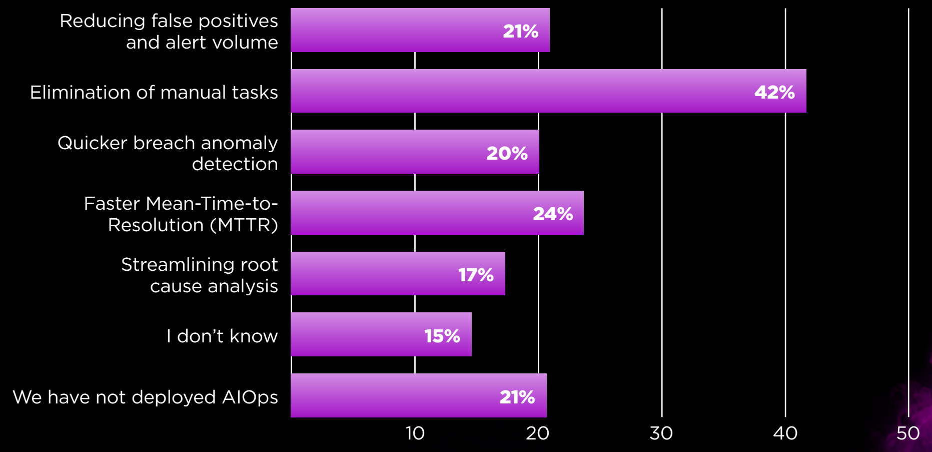
RISE OF AIOPS

AIOps goes mainstream with businesses of all sizes calling out deployment—nearly 8 in 10 have done so to date. Reinforcing the adage "junk in, junk out", the survey called out "data quality" as the biggest AIOps concern, followed by "skills gap"."Elimination of manual" tasks is cited as the top benefit of using AIOps tool, which is in alignment with the IT goal of automating operations and anomaly troubleshooting to streamline processes. The next highest was reducing Mean Time to Repair (MTTR).

What are your top 2 concerns about the use of AIOps Tools?



What are the top 2 primary benefits of using AIOps tools in your organization?



KEY TAKEAWAYS

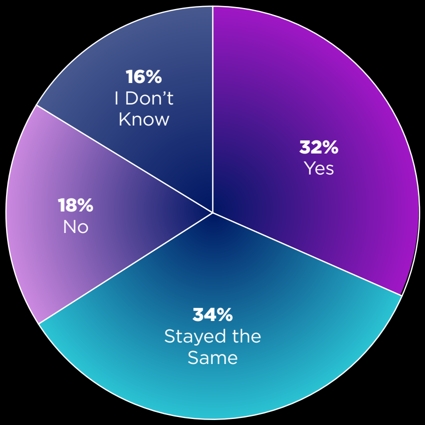
The survey suggests that AIOps is not a nascent technology but has become mainstream with adoption by a clear majority across all organization sizes. This growth is reflective of IT's goal in automating manual tasks to drive operational excellence. However, given concerns about data quality and the skills gap associated with AIOps, IT must make the most of the volumes of data captured. Finding professional talent to fill the skills gap continues to be difficult. We expect an increased demand for data scientists to make sense of the AIOps data.

IT BUDGETS UNCERTAIN

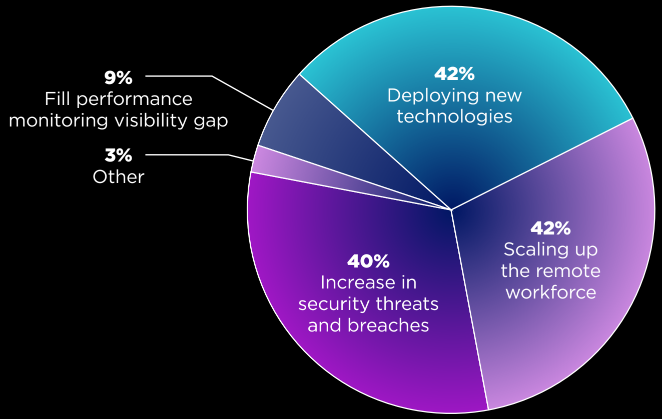
Even with the current economic head winds, most IT teams are reporting static or increasing budgets.

As shown elsewhere in the results, remote working is a primary driver of IT budget requirements along with cybersecurity threats and deployment of new technologies.

Is there a planned increase in your department's budget within the next 12 months?



What is the biggest driver of the budget increase?



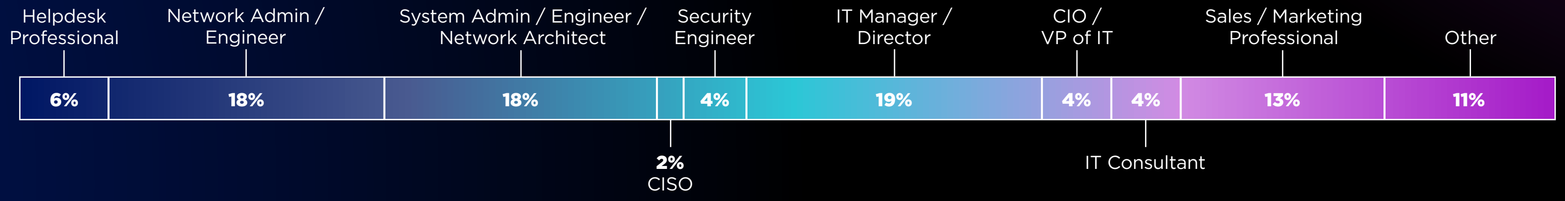
KEY TAKEAWAYS

Despite current market conditions, these budget projections are relatively upbeat. This could reflect a growing recognition by executive management of the importance of maintaining a robust network infrastructure even if it requires consistent or additional IT spend. That said there is still a need to more with less, as IT budgets are impacted by disruptions such as the remote work transition, security breaches, or new technology deployments. Lastly, tools consolidation should be prioritized over niche tools to cover use cases across a variety of stakeholders including NetOps, SecOps, and DevOps.

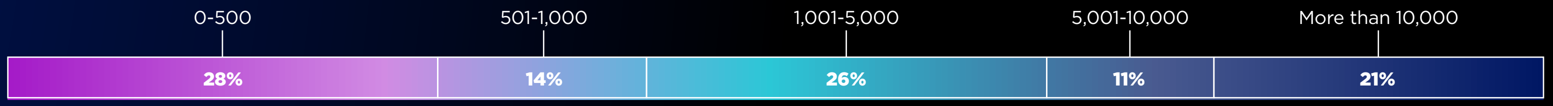
SURVEY METHODOLOGY

Survey questions were designed based on the needs and responsibilities of network and security professionals. Results were compiled from the insights of over 400 global respondents. In addition to geographic diversity, the survey population was distributed across multiple roles and industry verticals of different sizes.

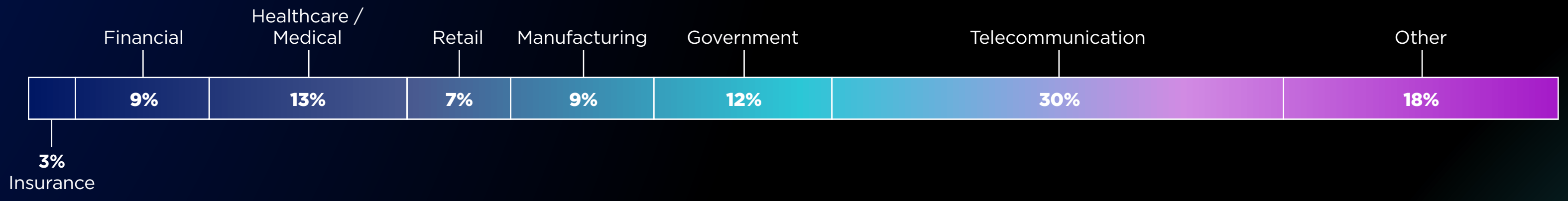
What is your primary job function?



How many employees does your organization have in total?



What is your primary market segment?



For more information about the survey methodology or the results, contact pr@viavisolutions.com.

Responses were collected in April 2020 via online surveys.

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

viavisolutions.com