STATE OF THE NETWORK

PERSEVERANCE

STATE OF THE NETWORK

VIAVI Solutions

STATE OF THE NETWORK

CONTENTS

FOREWORD BY SHAMUS McGILLICUDDY

VP of Research, Enterprise Management Associates (EMA)

The VIAVI State of the Network (SOTN) report has had its finger on the pulse of the world of network operations since 2007, when it was first published by the VIAVI Solutions corporate ancestor, Network Instruments. In fact, it's the only ongoing market research on NetOps that predates my own long running benchmarking research, EMA's Network Management Megatrends, which we first published in 2008. Like EMA, VIAVI has surveyed thousands of NetOps pros over the years about the issues that are impacting their professional lives. As in past years, the 2023 SOTN report reinforces and validates EMA's own research findings, particularly around the issues of network troubleshooting, unified communications and collaboration, and visibility into off-premises networks.

OFF-PREMISES (IN)VISIBILITY

First, the 2023 SOTN report found that network visibility into off-premises infrastructure is a major issue for network operations today. EMA wholeheartedly agrees. As of today, the cloud has absorbed at least 40% of enterprise application workloads that used to reside in private data centers. EMA research has found that only 18% of NetOps teams are fully satisfied with the visibility their tools provide into the cloud.

Furthermore, software-defined WAN has encouraged mainstream use of the public internet for corporate WAN connectivity, which presents new visibility challenges, since most SD-WAN solutions offer only limited insight into what's happening in the internet underlay.

Finally, the pandemic has created a work-from-anywhere revolution. Hybrid work is here to stay, and most of the NetOps pros I talk to are still trying to figure out the best way to get visibility into home office environments. Too many of them are relying on remote desktop access as a first line of defense, which simply won't scale.

END-USER EXPERIENCE: A CRITICAL KPI

This brings us to the SOTN finding that end-user experience is a critical KPI for NetOps. EMA concurs that this is something that network pros need to focus on, especially with the proliferation of hybrid work, real-time unified communications applications, and SaaS. NetOps can't focus on mean-time-to-innocence. "It's not the network's fault" won't solve the problem in an era when most enterprises are embracing digital transformation.

NetOps needs to help other IT groups connect the dots and solve end-user experience problems quickly. After all, EMA research has found that 31% of all problems that the NetOps team responds to were first reported by end users before the network team was aware of the problem. This means that 31% of all network problems ARE affecting end user productivity before the NetOps team even opens the ticket.

FIGHTING REAL-TIME COMMUNICATIONS FIRES

Speaking of end user issues, the SOTN report found that NetOps pros are spending more and more time troubleshooting problems with unified communications and collaboration apps. EMA is not surprised. The rise of work-from-home led to a cultural transformation in work life that relies heavily on real-time video and collaboration apps. Our research has found that nearly 95% of enterprises have seen increased traffic from real-time communications apps since the start of the pandemic. Even as people return to the office, this surge of real-time traffic will not subside. Network architects tell EMA they are building the next generation of on-premises office networks with this in mind, ensuring their Wi-Fi can handle the expected high-density, real-time app usage loads.

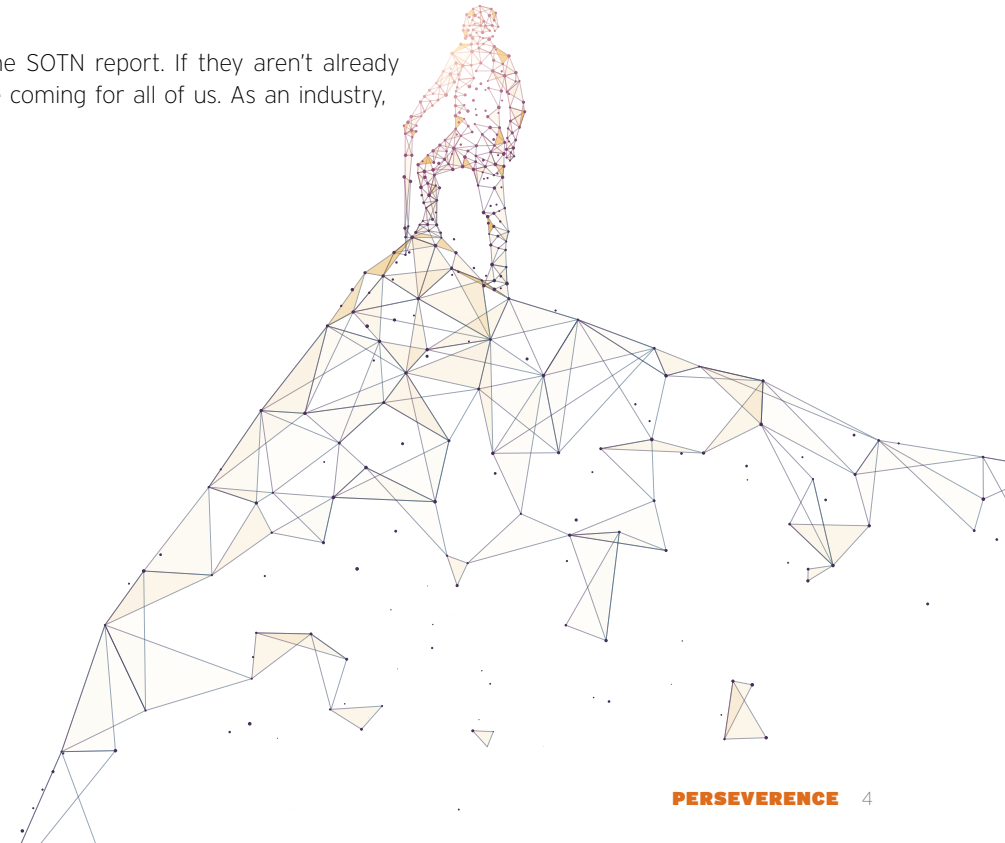
TROUBLESHOOTING PROCESSES ARE A MESS

Finally, the SOTN report has found significant dissatisfaction with network troubleshooting capabilities. Simply put, network pros struggle with root-cause analysis. One would think that after 30+ years, the network management industry would have figured this out by now. Unfortunately, much work remains to be done.

EMA's own Network Management Megatrends research recently found that only 28% of networking pros are fully satisfied with how their tools support root-cause analysis. A network architect at a large bank described it well to EMA recently: "Traditional tools are good at telling us that there is something going on and that we need to look at it, but there's a lot of manual troubleshooting after that. Tools are great for problem isolation, but not root-cause analysis."

In conclusion, NetOps pros should take a close look at the VIAVI findings in the SOTN report. If they aren't already dealing with the issues highlighted here, they will be soon. These challenges are coming for all of us. As an industry, we must solve them.

Shamus McGillicuddy is the VP of Research at Enterprise Management Associates (EMA), where he leads the network management practice. His research focuses on network automation, AIOps-driven network operations, multi-cloud networking, and WAN transformation.



EXECUTIVE SUMMARY

This year's 15th consecutive State of the Network (SOTN) revolves around themes of perseverance and resiliency. VIAVI believes these words capture well the efforts of IT teams to maintain reliable application delivery in the face of evolving challenges and rising user expectations since the first survey in 2007.

Results from the 2023 survey maintain this tradition of determination, capturing trends both new and several spanning back to the first report in 2007. For example, the initial report focused on VoIP rollout plans and the associated obstacles for network teams. Similarly, this year's report – among other things – asked about Unified Communications and Collaboration (UCC) solutions with conclusions that, though not identical, certainly are comparable.

In contrast, there are findings that few would have imagined in 2007. These have been called out over the intervening years, including persistent IT staffing challenges, the widespread acceptance of cloud-based technologies and services, complex hybrid multi-tier applications, and the incredible growth of cybersecurity threats to name a few. With each of these, IT teams have shown themselves to be flexible and able to adapt as required. This has probably been aided by greater collaboration between NetOps, SecOps, and DevOps groups. In addition, the advent of better tools has likely aided efforts here as well. The results are impressive; consistent, high levels of service delivery.

This is even more impressive with two other observations. First, users' expectations have grown enormously in this time frame, with IT stakeholders assuming they can connect anytime with others via solutions like MS Teams or use their smart phones to access applications anywhere. Second, to remain viable, businesses have come to completely expect mission critical services to be always available.

If the next 15 years are anything like the last 15, IT teams responsible for maintaining peak network and application performance can likely expect little letup in ongoing and new operational hurdles. That said, history suggests they have the fortitude, creativity, and wherewithal to keep users happy and businesses running smoothly well into the future.

TOP FINDINGS

1. **THE HAMSTER WHEEL OF NETWORK APPLICATION TROUBLESHOOTING** Despite 15 years, and billions of dollars of investment*, IT network managers are far from understanding the source of the issues that plague their network, according to the State of the Network 2023 study conducted by VIAVI. Respondents in 14 of the past 15 years—including 2023—have called out "problem domain isolation" (root cause analysis) as the top challenge. According to the IT professionals polled, the way out of this is clear: Measuring and delivering a great end-user experience is an IT network manager's top metric in 2023 in a remote-first, cloud-native modern enterprise.

2. **FAILING TO COMMUNICATE** VoIP and other real-time services remain a big headache for IT teams. In the very first survey in 2007, it was VoIP service. In 2023, nearly 50 percent call out spending between 10 and 20 hours troubleshooting unified communications and collaboration platforms. This issue falls mostly on the NetOps team to resolve. Given the importance of collaboration and communications in today's fast moving world and the heavy troubleshooting workload, more needs to be done to reduce UCC problem triaging and resolution burdens.

3. **CLOUD & OFF PREMISES MODERNIZATION IS THE ANSWER AND THE PROBLEM** Of the top five visibility challenges called out, four are tied to cloud or off-premises assets. Despite this it's full-speed ahead for cloud deployments. 70 percent reported that more than half of their applications and services are hosted in the cloud. Compare this to 2018 where only 10 percent did so. Even conservative NetOps teams are all-in on the cloud, with nearly 70 percent reporting plans to move between 51 and 75 percent of their services to the cloud within the next two years.

4. **IT'S EXPENSIVE, BUT IT'S WORTH IT** Eighty percent of network managers report that savings from cloud modernization exceeded predictions and 83 percent state that the benefits outweighed the cost.

5. **THE USER EXPERIENCE IS THE ONLY THING THAT MATTERS** When respondents were asked which was the most important of their monitoring objectives, the need to understand end-user experience rose to the top, surpassing other packet, flow, or active test-based metrics. Seven in ten stated it was "very important." This applied whether tied to IT delivery strategies, cloud monitoring objectives, data center rollouts, and overall project budget considerations. The data confirms that monitoring teams should focus on acquiring or improving end-user experience intelligence to improve their efficacy.

6. **DO WE NEED MOORE'S LAW OF NETWORK GROWTH?** The growth in the amount of data flowing in today's networks is mind boggling with little sign that it is abating. No matter how big the network pipes get, users have an insatiable urge to keep "filling them!"

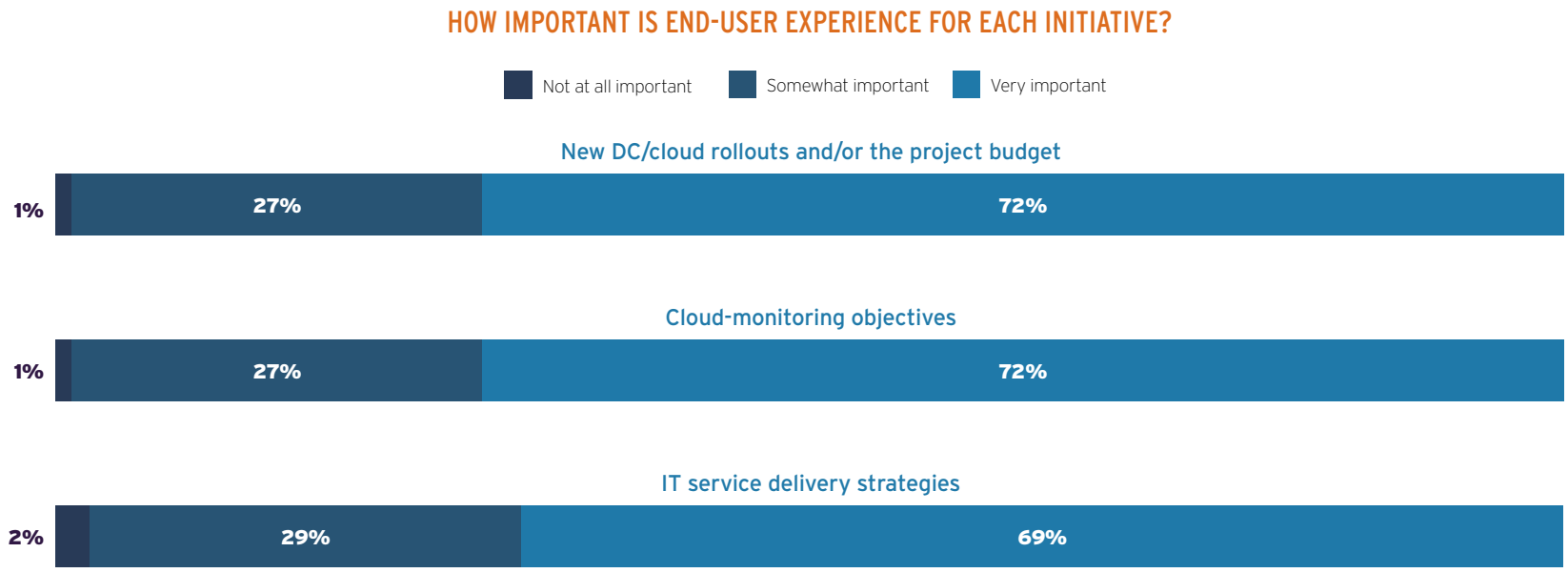
7. **IT TEAMS FLYING BLIND WITH TLS ENCRYPTION** Cybersecurity vulnerabilities and application troubleshooting escalate with increasing rollout of TLS.

*Gartner estimates that the size of the worldwide NPM market in 2021 will be approximately $2.7 billion, growing at a compound annual growth rate (CAGR) of 5.1% through 2024. *Gartner Market Guide for Network Performance Monitoring,* Published 9 August 2021 - ID G00749249

THE IMPORTANCE OF END-USER EXPERIENCE AWARENESS

BEATING OUT OTHER METRICS TO CLAIM TOP SPOT

In this year's survey, when asked which was the most important of their monitoring objectives, respondents stated the need to understand end-user experience as their top choice. This surpassed all other packet, flow, or active test-based metrics. **Seven in ten stated end-user experience awareness was "very important."** Nearly 3 in 10 said it was "somewhat important."

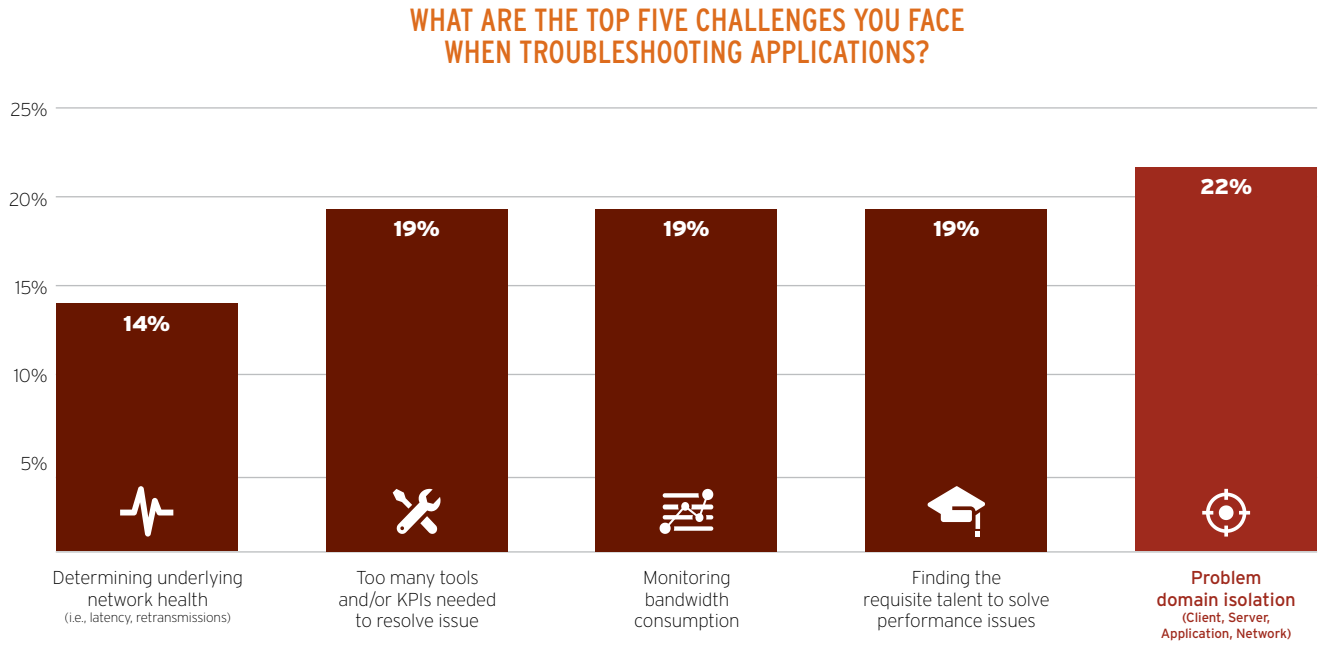


End-user experience intelligence is critical to delivering peak IT services, providing deep insights into the satisfaction and productivity of users while serving as an excellent metric to gauge the underlying health of network resources.

TROUBLESHOOTING OBSTACLES

PROBLEM ISOLATION MAINTAINS TOP SPOT

Problem domain isolation / locating the source of an issue remains the top troubleshooting issue for IT teams. In past SOTN surveys, VIAVI has asked a similar question. Each time, except in 2021, domain isolation was selected as the biggest challenge. Advances in monitoring tools or KPIs appear offset by new difficulties, whether IT staffing issues, more service delivery methods, or new underlying supporting technologies.



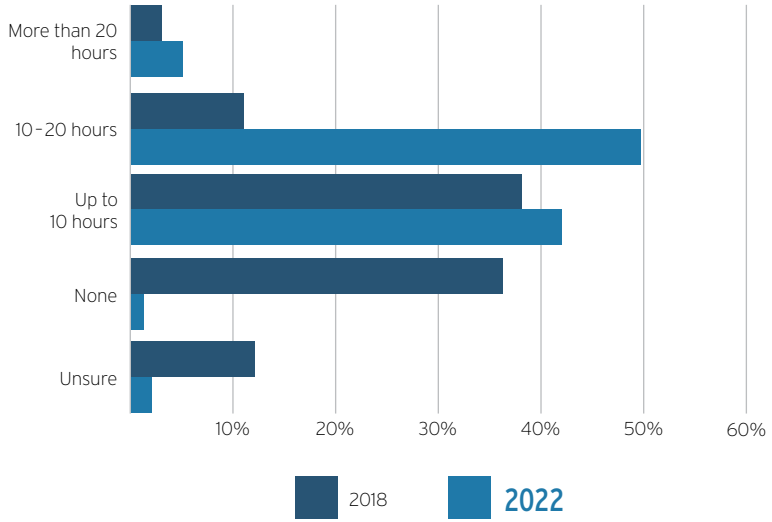
Technologies come and go, new services are added or removed, and application complexities increase. The one constant: problem domain isolation remains the biggest problem for IT teams.

TROUBLESHOOTING OBSTACLES

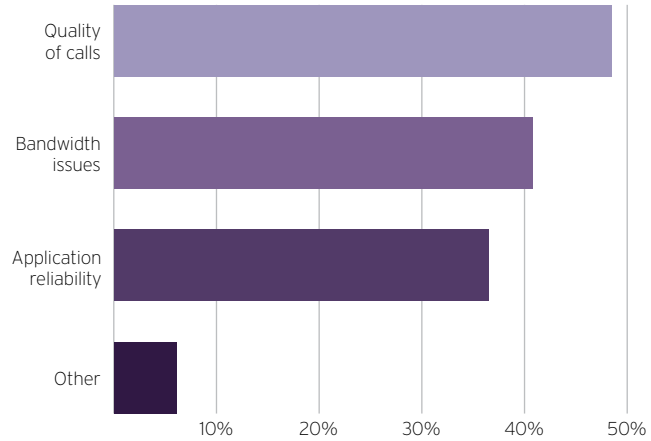
UNIFIED COMMUNICATIONS AND COLLABORATION WOES INCREASE

Since it's introduction with VoIP in the late 90s, the real-time nature of unified communications (UC) has been a persistent challenge for IT network teams. The introduction of video and collaboration (UCC) tools has increased the headaches, as can be seen with this year's survey results. Comparing previous survey findings from 2018 to 2022 vividly illustrates how IT teams are spending more time troubleshooting, especially for those calling out greater than 10 hours per week with nearly 50 percent specifying between 10 and 20 hours per week. Deeper data breakouts show NetOps teams are really being stressed on this, much more than SecOps and DevOps. For historical perspective, also included below are results from the first SOTN survey in 2007, where the question focused on VoIP.

HOW MANY HOURS PER WEEK DO YOU SPEND TROUBLESHOOTING UNIFIED COMMUNICATIONS (UCC) ISSUES?



WHAT ARE YOUR PRIMARY VoIP CONCERNS?



Results from the 2007 SOTN survey

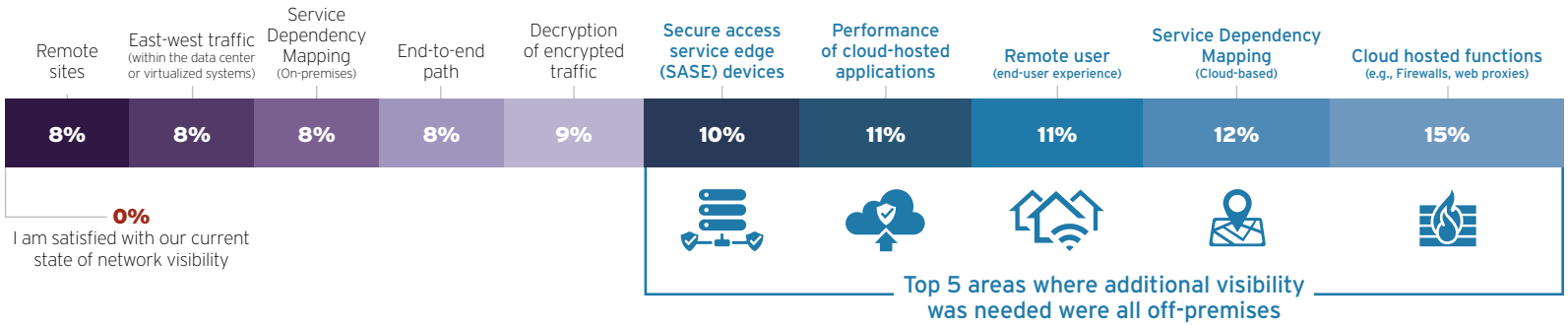
NetOps teams are being overwhelmed with UCC troubleshooting, spending significant amounts of time resolving issues – they need better tools to aid in this effort sooner rather than later.

IT TEAMS NOT SATISFIED WITH CURRENT NETWORK VISIBILITY

The concept of "network visibility" is in the news more often recently. Though definitions sometimes vary, VIAVI defines it as: "*The IT team's ability to monitor the state of the network, including users, applications, data and transactions, in order to anticipate, prevent, troubleshoot, and resolve issues before they affect productivity and business results.*" This year we asked where there was a need for more visibility. Two results stood out:

1. **The top 5 areas where additional visibility was needed were all off-premises** – you can see them called out below – these disparate outsourced IT assets may aid initiatives related to business efficiencies but are detrimental to service status awareness and intelligence.
2. **Only two respondents out of more than 300 were satisfied with their levels of visibility.**

Further data analysis shows DevOps are more likely to say they invested in new tools to get cloud visibility. Upon reflection, this makes sense as DevOps are not as likely to use "network centric" tools and instead utilize alternative solutions. This is backed up by EMA research, where their stated preference is for APM/DevOps observability tools. NetOps may have offered their legacy tools and DevOps said "no, we're buying our own stuff."



There are high-levels of dissatisfaction with network visibility. Cross-demographic results show this was a consistent theme spanning department, title, and industry vertical.

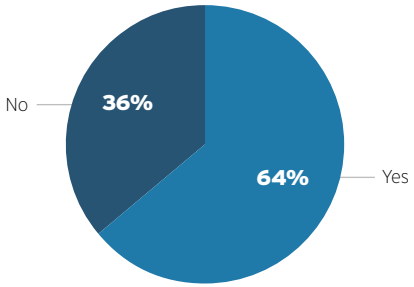
IT TEAMS NOT SATISFIED WITH CURRENT NETWORK VISIBILITY

WITHOUT ADVANCED PLANNING TLS ENCRYPTION HAMPERS EFFORTS

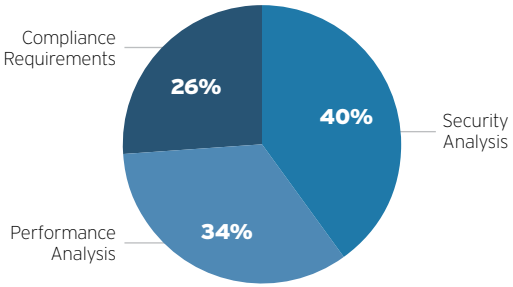
The process of making a network more secure via encryption can greatly reduce visibility into what's traversing the environment as packet payload is unavailable without access to the private key to decrypt. This year's survey asked, "Do you have a requirement to decrypt captured packets in your environment?" Nearly 2/3 stated they have this requirement.

Specific use cases for decryption were highlighted as well. "Security analysis" was called out the most at 40 percent, with "compliance requirements," in third place at 26 percent. Somewhat surprising to VIAVI was that "performance analysis" was indicated at 34 percent, suggesting that many network monitoring teams still need access to decrypted data for service performance assessments. Further analysis showed strong interest by all teams, with a particular emphasis from SecOps, less so for NetOps and DevOps. Lastly, the demand for visibility to traffic spanned both on and off-premises.

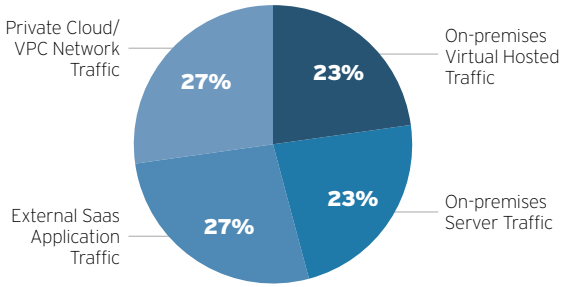
DO YOU HAVE A REQUIREMENT TO DECRYPT CAPTURED PACKETS IN YOUR ENVIRONMENT?



WHAT ARE YOUR USE CASES FOR WHICH DECRYPTION IS REQUIRED?



IN WHICH ENVIRONMENTS DO YOU REQUIRE DECRYPTION?

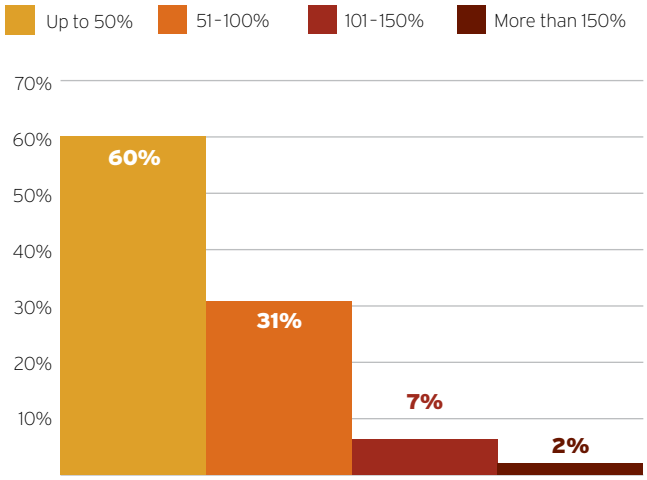


Access to traffic details via comprehensive network visibility is a must for SecOps—encryption materially impacts visibility. NetOps and DevOps teams also expressed interest but not as great as SecOps. This highlights the need to balance privacy with robust cybersecurity intelligence, and IT service health/status visibility.

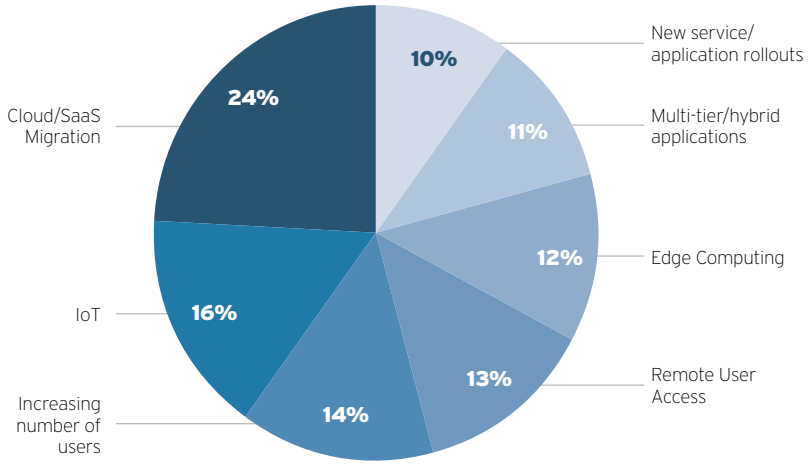
BANDWIDTH GROWTH & DRIVERS: TODAY

Bandwidth growth shows no signs of slowing. This year's respondents called out "up to 50 percent growth" 60 percent of the time, with another 31 percent indicating "51-100 percent." The remaining 9 percent reported expected bandwidth increases of more that 101 percent. What's driving this increase is multifaceted. Topping the list was cloud/SaaS migration at 24 percent, with IoT and increasing number of users second and third, respectively. It's notable that a lot more user traffic goes off-prem than in the past. This requires more WAN/internet bandwidth. Beyond SaaS moving applications off premises, desktop solutions such as O365 creates even more demand on the network. It's also important to note that each of the remaining drivers reported double-digit contributions to bandwidth increases.

HOW MUCH DO YOU EXPECT BANDWIDTH DEMAND TO GROW IN THE NEXT TWO YEARS?



WHAT ARE THE DRIVERS OF INCREASING BANDWIDTH DEMAND?

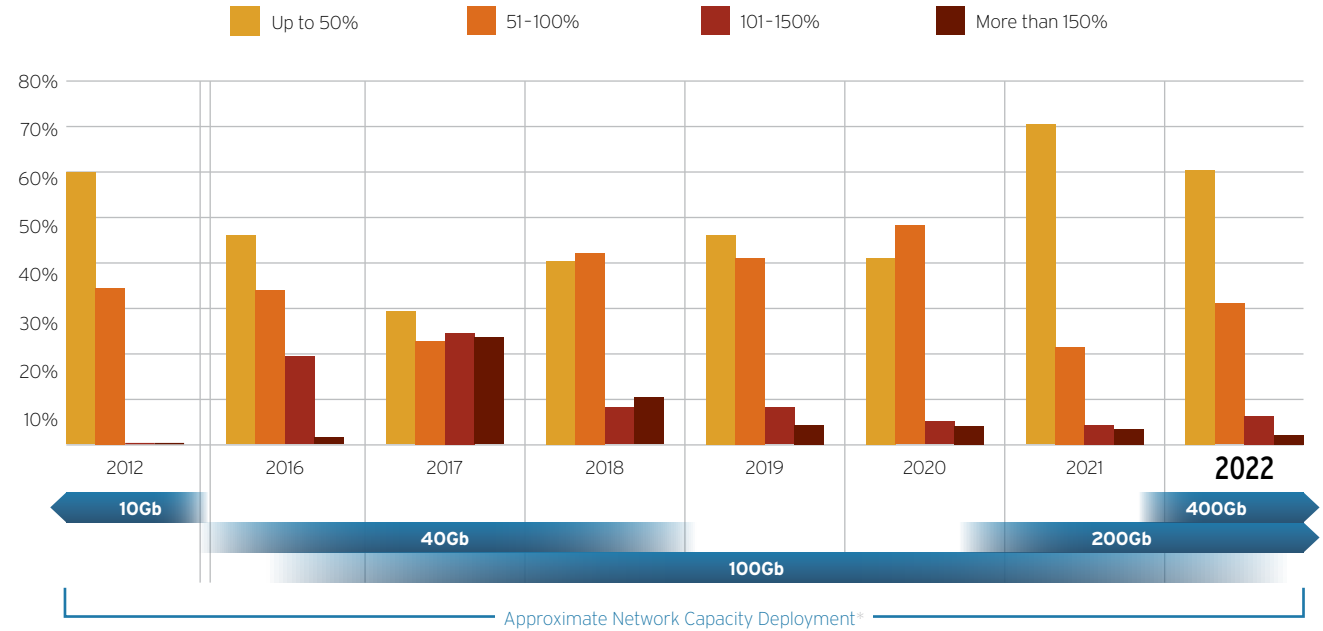


A well functioning network infrastructure can maintain peak operational efficiencies only when there is sufficient bandwidth to support new initiatives and/or escalating demands whatever the ultimate driver of the increase.

BANDWIDTH GROWTH & DRIVERS: A HISTORICAL PERSPECTIVE

Here's a ten-year time horizon of bandwidth growth. Look at 2012 results where there were similar increases expected for the same growth ranges as reported in 2022. What's missing is a perspective on how much more capacity has been deployed in the same timeframe. The second timeline below the bandwidth graph vividly illustrates this increase.

HOW MUCH DO YOU EXPECT BANDWIDTH DEMAND TO GROW IN THE NEXT TWO YEARS?



The growth in the amount of data flowing in today's networks is mind boggling with little sign of slowdown. Organizations will need to keep making investments in their network resources to keep up with the data deluge.

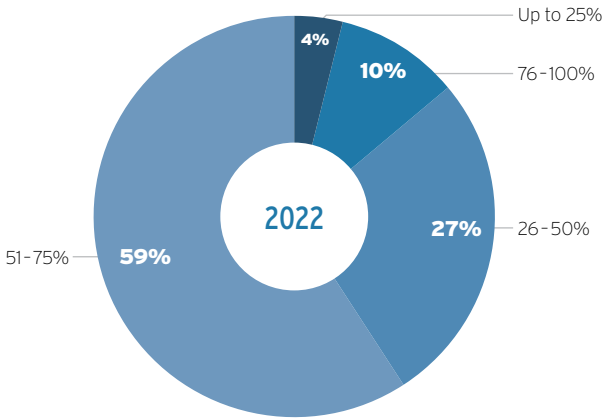
*This timeline is designed to convey the approximate introduction and life cycle for network capacity listed for a "typical" enterprise. It is based on transceiver revenue and is a combination of data center, data center interconnect, and cloud deployments. Source beginning with 2016: *LightCounting Ethernet Transceivers Forecast September 2022 High Speed Ethernet Optics Report Forecast* published September, 2022.

BUSINESS IS BULLISH ON CLOUD DEPLOYMENTS

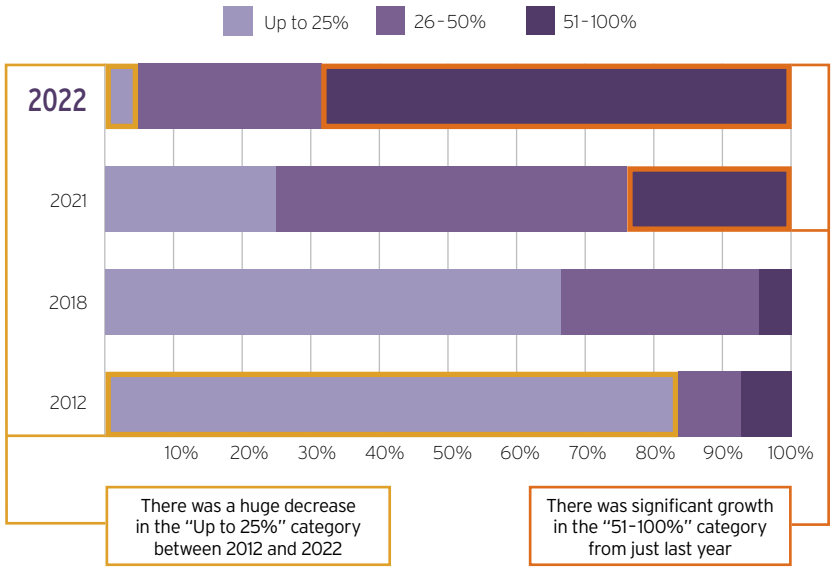
Going into this year's survey, we were not certain how growth in cloud deployments would be reported. Why? Because, though there are many benefits of cloud-hosted services, there was also more news suggesting businesses were growing increasingly frustrated with cloud deployment downsides. This year's survey shows business embracing migration with little evidence of this counter trend of cloud deployment concerns. Results show nearly 27 percent indicated up to 50 percent of applications and services are cloud hosted with another 59 percent calling out 51 to 75 percent. More than 10 percent have up to 100 percent in the cloud.

Compare these findings and note the call-outs illustrating the dramatic change in ten years from 2012 to 2022.

WHAT PERCENTAGE OF APPS ARE CLOUD-HOSTED?



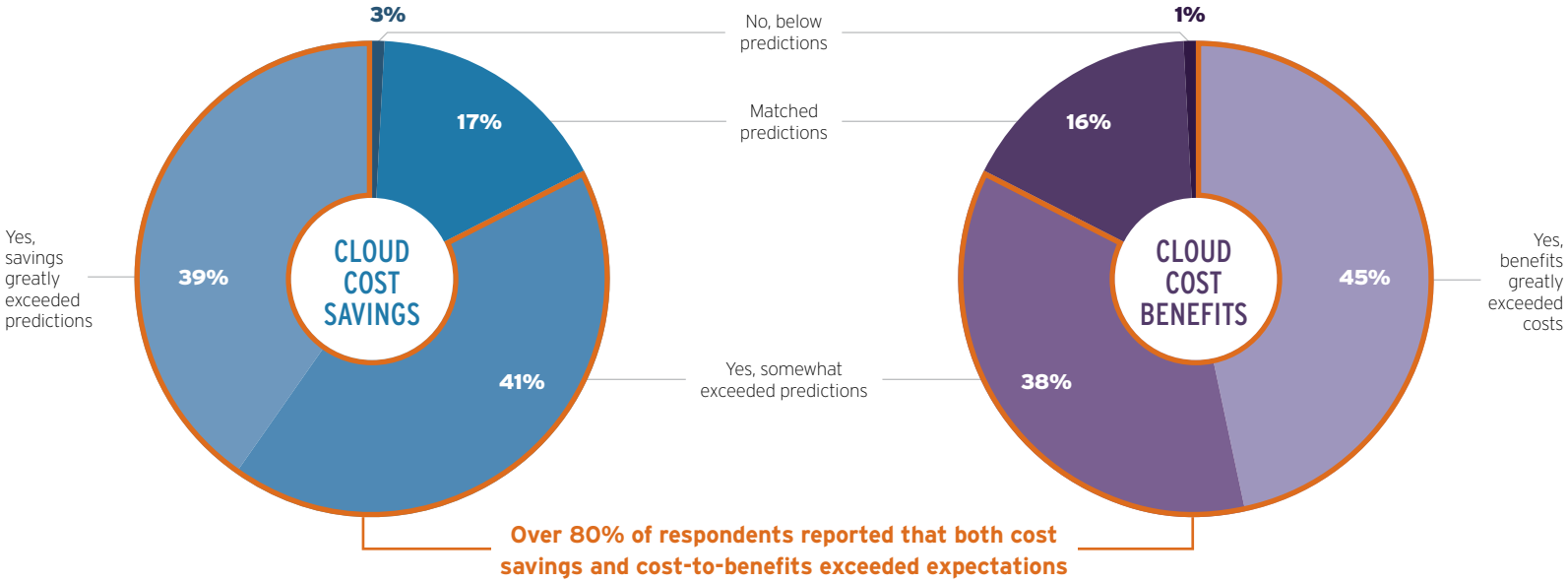
CLOUD HOSTING GROWTH OVER THE YEARS



The verdict on cloud hosted applications and services is in—any lingering concerns about migration are quickly disappearing. This years' SOTN respondents are accelerating their cloud migration activities like never before.

CLOUD MIGRATIONS DELIVER ON COSTS SAVINGS AND BENEFITS TO BUSINESS

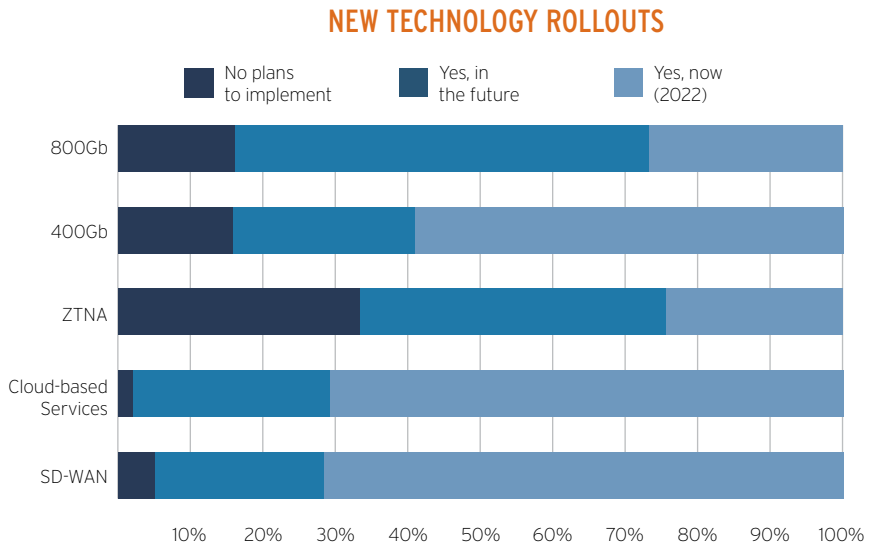
The acceptance of cloud for application and service hosting reported in this year's survey appears completely justified based on respondents' feedback regarding cost savings and benefits. Eighty percent stated actual cost savings of migrating to the cloud either somewhat or greatly exceeded predictions. Meanwhile, 83 percent responded that predicted benefits of cloud migration outweigh the transition and ongoing costs. Only one respondent out of 308 was negative about cloud.

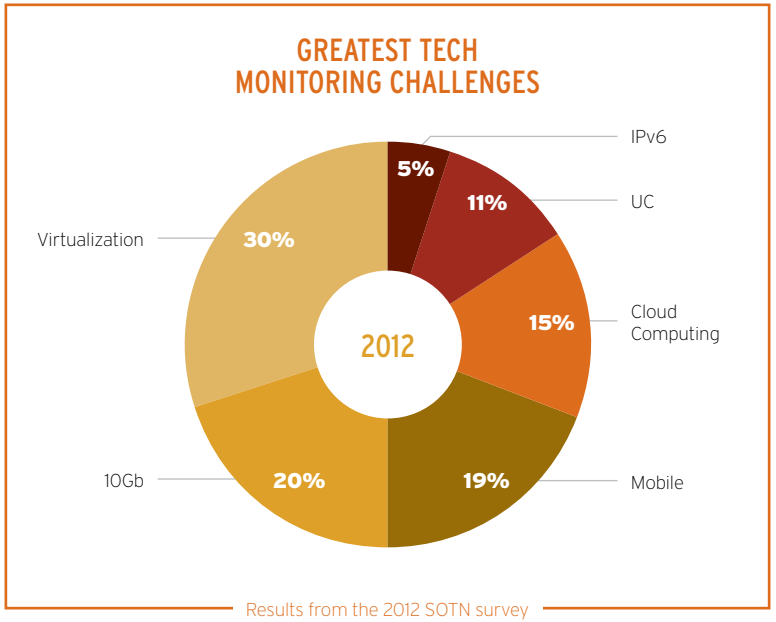


Business and IT teams are overwhelmingly satisfied with the value gained by cloud hosting.

NEW TECHNOLOGY DEPLOYMENT PLANS REMAIN STRONG DESPITE ECONOMIC HEADWINDS

Rising interest rates and economic uncertainty has not significantly dimmed the outlook for IT teams' technology spend. As called out elsewhere in the report, organizations reported large benefits and cost savings with cloud-based services. This bullish sentiment is confirmed in deployment plans, with more than 97 percent planning cloud rollouts by 2024. SD-WAN is also clearly delivering business value, coming in strong at 95% through 2024. Reviewing Zero Trust Network Access (ZTNA) current and planned adoption suggests organizations are fine (at least for now) with legacy VPNs with ZTNA being rolled out more slowly. Finally, both 400 Gb and even 800 Gb networks showed surprising growth expectations. Compare these findings with results from 2012 where the only overlap with today is "cloud computing."





Results from the 2012 SOTN survey

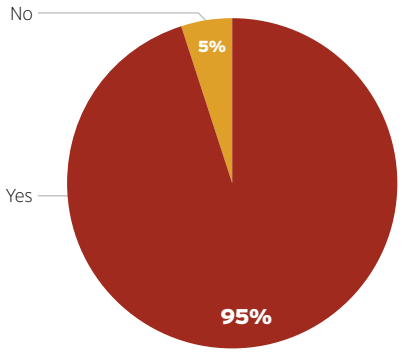
Those responsible for IT infrastructure spending have big plans for technology rollouts. IT teams involved in performance monitoring and cybersecurity must ensure they maintain sufficient network visibility as underlying technologies evolve.

CYBERSECURITY THREATS

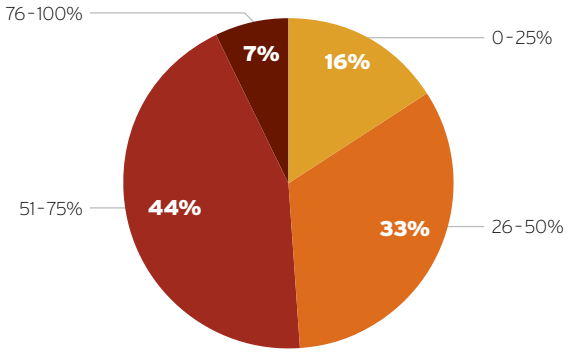
IT TEAMS MITIGATION EFFORTS ESCALATE

This year's survey shows there is no let up for IT teams with cybersecurity threats increasing. When asked "Is your organization's IT team involved in resolving security issues?" 95 percent said "yes." Important to note here, the more detailed data shows 97 percent of NetOps teams and 88 percent of DevOps groups are involved, so this is an enterprise-wide problem. Compare to the State of the Network 2017 survey, when 88 percent answered similarly. Digging a bit deeper into this year's data, the amount of time spent on security concerns is also materially growing. Those calling out 26 to 50 percent of their time went up from 30 to 33 percent, while the segment "more than 51 percent" increased from 47 to 51 percent. Network teams need to work more closely with security teams to make sure they are efficient in resolving security issues. Complicating matters, if network teams are too caught up in security activities, they may fall behind on their strategic projects.

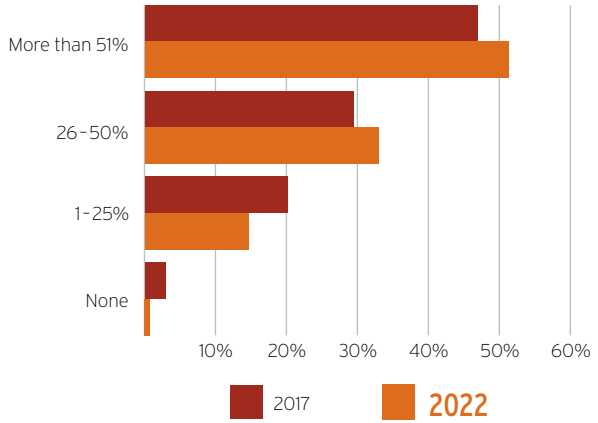
IS YOUR IT TEAM INVOLVED IN RESOLVING SECURITY ISSUES?



HOW MUCH TIME IS SPENT PER WEEK RESOLVING SECURITY ISSUES?



TIME SPENT ON SECURITY 2017 vs 2022



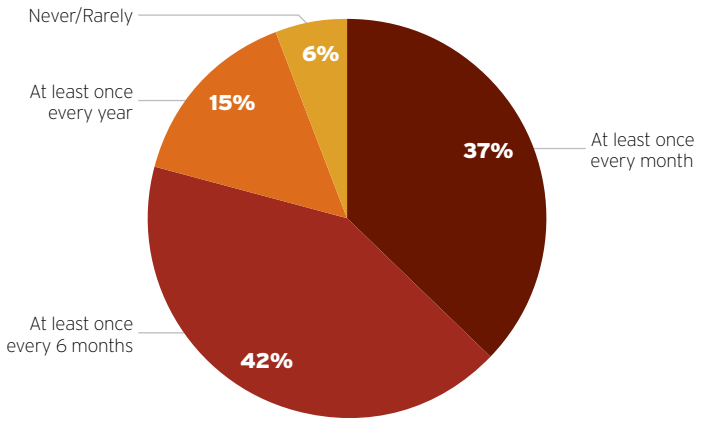
Close collaboration between NetOps and SecOps teams is a must in a world of a never-ending cybersecurity threat horizon. The constant drum beat of cybersecurity breaches in the news translates into large amounts of time being spent by IT teams on a daily basis. Whether preventing, detecting, or resolving post-breach events, staff are stretched thin as they balance the need to address cyber threats while still maintaining adequate application and service delivery levels.

WAR ROOM SCENARIOS ARE ON THE RISE

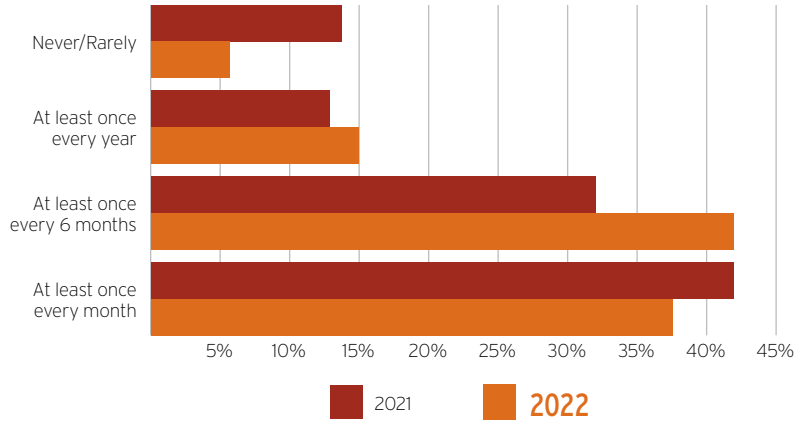
The combination of troubleshooting activities with an increasing amount of cybersecurity responsibilities translates into tons of work for IT teams. For 2023, 37 percent of respondents stated they have "war room" events "at least once a month." In 2021, 42 percent specified "at least once a month."

Notably, SecOps is being pulled into the war room much more often than NetOps. DevOps is also required more frequently than in the past. This might suggest that cloud migration is driving more war room responses, and the network team doesn't get involved because they have limited visibility.

HOW OFTEN DOES YOUR ORGANIZATION MEET IN THE "IT WAR ROOM" TO SOLVE A DIFFICULT PROBLEM?



IT WAR ROOM MEETINGS 2021 vs 2022

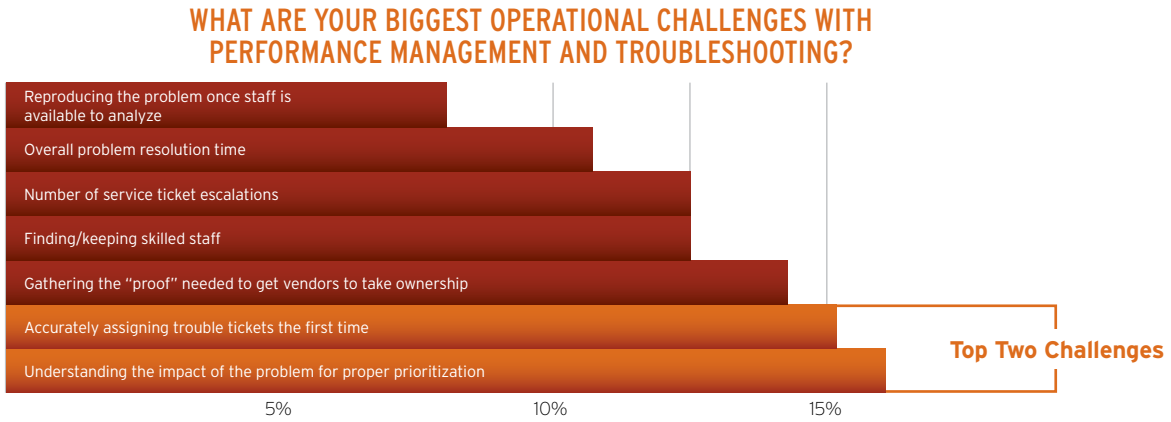


War room events can consume vast IT team resources. Results for the past two years show only minimal improvement. Because many current tools aren't making it clear where the problems reside, the time and resources needed to maintain the network, optimize the applications, and contend with cybersecurity threats are growing. IT teams should target solutions that automate the domain isolation process and accelerate root cause identification.

OPERATIONAL CHALLENGES MULTIPLY IT TEAM STAFFING HEADACHES

When it comes to operational challenges, two of the top three concerns "Understanding the impact of the problem for proper prioritization" and "Accurately assigning trouble tickets the first time" speak directly to the capabilities of the network performance monitoring solution in place. It also ties well with concerns mentioned within the "Troubleshooting" realm, where "domain isolation" is consistently listed as the most frequent challenge.

Complexity is a prime driver here – evolving technologies as well as application and service rollouts. Adding to this is customer user experience expectations, which continue to grow. IT teams need the right information, presented in the right format as near real-time as possible to stay ahead of issues.



This year's survey has called out numerous difficulties for IT teams, whether operational, related to troubleshooting, or addressing cybersecurity challenges. Automation initiatives planned or underway suggest that expected benefits could offer significant relief to struggling staff.

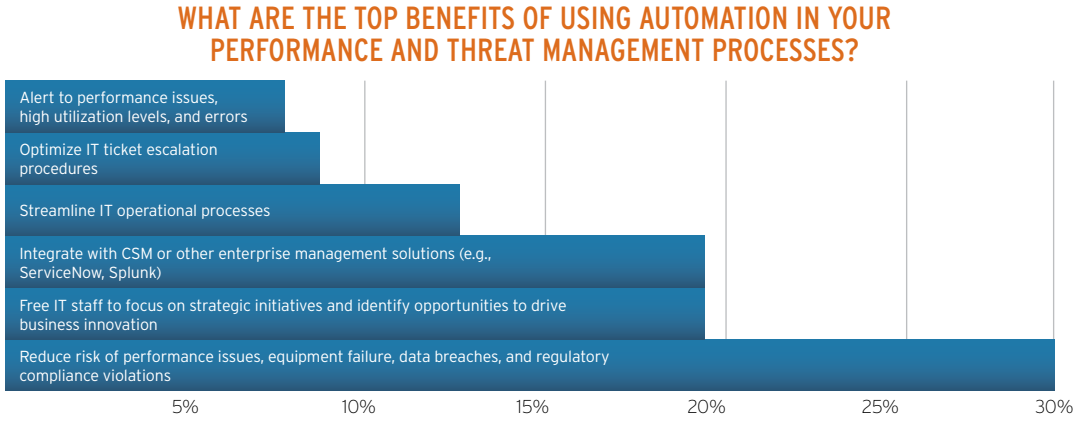
AUTOMATION MUST BE A PRIORITY FOR IT TEAMS

Respondents, by a wide margin, stated the largest benefit for automation was "Reduce risk of performance issues, equipment failure, data breaches, and regulatory compliance violations." Any of these can wreak havoc on the smooth operations of IT services, expose the organization to governmental sanctions, or increase negative customer sentiment

Also called out was "Free IT staff to focus on strategic initiatives and identify opportunities to drive business innovation" and "Integrate with CSM or other enterprise management solutions (e.g., ServiceNow, Splunk)."

The former aligns very well with the operational challenges, troubleshooting headaches, and too-frequent "war rooms" scenarios discussed elsewhere in this report. More importantly, it gets IT teams out of the rut of spending most of their time on tactical issues only and enables them to think about longer-term initiatives that can aid business.

The latter speaks to the importance of sharing network data with larger third-party platforms which automate incident management and can be significant time savers.



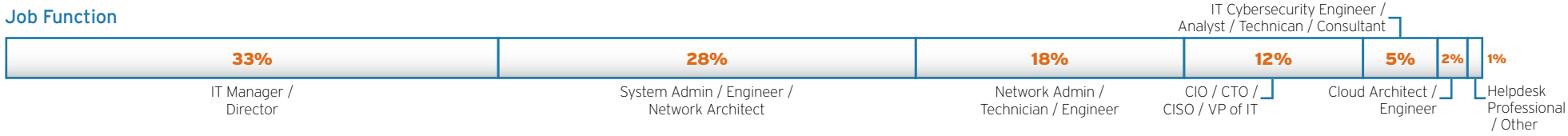
It is incumbent that IT makes automation efforts a top priority. If for no other reason, they are likely to be (eventually) buried in day-to-day IT performance issues and security breach remediation "skirmishes" with no relief for over worked, struggling staff.

SURVEY METHODOLOGY

The insights from this report were based upon a survey of network, security, and development operations professionals. Results were compiled from the insights of 307 respondents from around the world. In addition to geographic diversity, the study population was distributed by age, industry experience, current level, job function, department, revenue, employee count, and business verticals.

Location

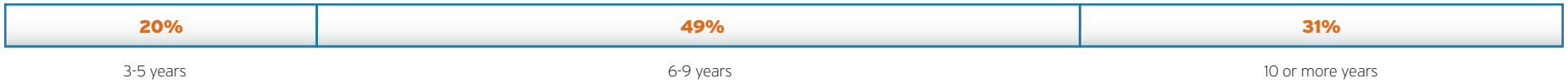
Job Function



Annual Company Revenue

Industry Segment

Industry Experience



For more information about the study's methodology or the results, contact sonus@pr.com

To see VIAVI Observer in action, please visit viavisolutions.com/observerdemo. Responses were collected in September 2022 via an online survey.

stateofthenetwork.com

STATE OF THE NETWORK

VIAVI Solutions

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

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

sotnreport-perserverance-wp-ec-nse-ae
30193634 900 1222