CLOUDBRINK

2025 TRENDS IN HYBRID WORK REPORT

The Facts Behind Balancing Security and Performance

CONTENTS

Executive Summary: Hybrid Work Is On Target, but Secure Access Strategies Miss the Mark 3

Part I. Remote Work Is Now Just Work — Organizations Secure Access In Nearly Every Way 11

Part II. Security Gets Selected Over Performance, But What If You Could Have Both? 14

Part III. Problems Persist as Traditional SASE Fails to Fix Performance Issues 17

Part IV. Businesses Plan to Invest But Traditional Approaches Don't Deliver. 22

Appendix. 28

EXECUTIVE SUMMARY

HYBRID WORK IS ON TARGET, BUT SECURE ACCESS STRATEGIES MISS THE MARK

New research suggests companies' growing fears about hybrid work are unfounded, but that hidden dangers lie elsewhere. While some organizations fear work-from-anywhere employees may put in less time than those sitting in physical offices, data suggests they work longer and harder.

On the other hand, IT professionals universally underestimate the impact of security solutions on business performance and user experience. Participants overlook the significant impact that packet loss has on application performance and, therefore, user productivity, particularly when combined with the latency introduced by security tools.

Without a clear grasp on what's causing poor performance, IT professionals continue to apply costly, misguided and ineffective strategies to fix application issues and reduce operational complexity.

Trends and Conclusions

- Hybrid employees work longer hours
- IT and security leaders underestimate the impact of packet loss on performance
- With the exception of modern Personal SASE, remote access solutions such as VPN, ZTNA and SASE do not solve the problem
- Organizations find new solutions like traditional SASE hard to manage and support
- Most companies plan to invest in swapping out or supplementing solutions—but aren't sure how

Key Findings

51.3%

Remote work is now just work. More than half of all respondents say 40% or more of their employees work remotely at least one day each week.

69.3%

Realize their organizations' security capabilities negatively impact performance. However, findings suggest professionals don't understand the full impact or how to fix it.

82.5%

IT and security professionals don't understand the significance of packet loss — the #1 culprit for the loss of work-from-anywhere productivity. Packet loss is often overlooked, along with the solutions available to mitigate its damaging effects.

29.5%

Organizations lack the ability to consistently pinpoint the source of performance issues. As a result, the fixes IT professionals are most likely to apply do not align with the underlying causes of performance problems.

78.5%

Maintaining and supporting current remote access solutions is demanding and resource intensive. Respondents also find solutions cumbersome and costly to roll out.

94%

Virtually all organizations plan to invest in improving or upgrading their secure remote access solutions. One-quarter plan a complete replacement within 12 months.

Keep reading to see how your organization stacks up against industry peers and uncover ways to:

- Fix the flaws in solutions like VPNs, ZTNA, SASE and VDI
- Minimize the effects of packet loss and security tool-induced latency to enhance application performance and boost employee productivity
- Improve ROI and lower staffing costs with Personal SASE
- Reduce operational overhead so valuable support and security teams can focus on higher priorities

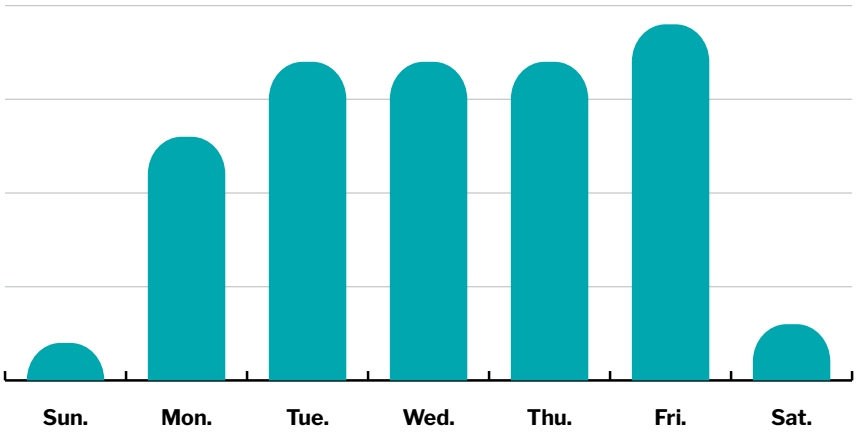
Where did we get this data?

This report features real usage data from millions of sessions a day from hybrid workers combined with a survey of 251 IT/network (57.8%) and cybersecurity (42.2%) professionals from a broad range of industry sectors. More than half of all participants in the survey work at companies with 5,000 employees or more.

Work-from-anywhere does not result in shorter working hours

Instead of jumpstarting long weekends as employers might fear, Cloudbrink usage data shows heavy transfer of data on Fridays, an indication that 'work from anywhere' employees actually put in *longer* hours than their '9 to 5' counterparts — with heavier usage starting at 7 AM and continuing to 7 PM. Trend data suggests remote workers continue transferring data on Saturdays and Sundays as well.

Global Traffic through Cloudbrink Service



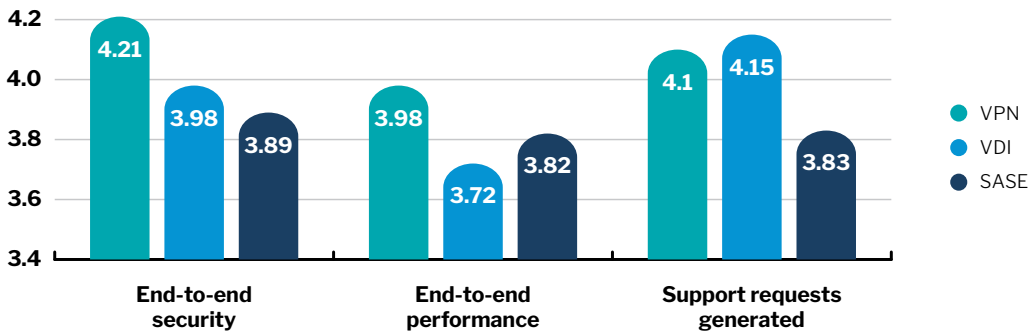
Secure access solutions can't meet goals for performance

Even those who use Secure Access Service Edge (SASE) as their main solution reported below-average satisfaction with its end-to-end security and performance. They also expressed dissatisfaction with the number of support requests generated by their secure remote access strategies. Findings suggest investments in modern secure access solutions like SASE and zero trust network access (ZTNA) fail to deliver businesses' sought-after benefits.

SASE vs. Personal SASE

Where traditional SASE predominately improves the performance of SD-WAN connections to office locations, **Personal SASE** enhances performance wherever users are located — where experts say most performance issues arise. Personal SASE combines **High-performance ZTNA** with **Automated Moving Target Defense (AMTD)** and Personal SD-WAN to mitigate the impact of packet loss, centralize visibility, and streamline secure access from any location.

Satisfaction with Remote Access Capabilities



Companies fail to recognize the impact of packet loss on ROI, performance, and productivity

As businesses continue to prioritize remote work security ahead of performance, IT and security professionals are aware but don't fully understand how security impacts user experience — and what can be done about it.

Packet loss devastates performance

Cloudbrink data and research by the US Department of Energy's **Energy Sciences Network** show the negative impact of packet loss on performance is exacerbated by latency — often introduced by security solutions. ***Adding just .005% packet loss on top of just 10 milliseconds of latency can cause throughput to plummet by 90%.***

SASE and ZTNA solutions often add up to 100msec of latency which in the presence of packet loss can reduce the effective throughput of a 100Mbps or 1Gbps connection to just a few Mbps.

More secure but less satisfied

86.9%

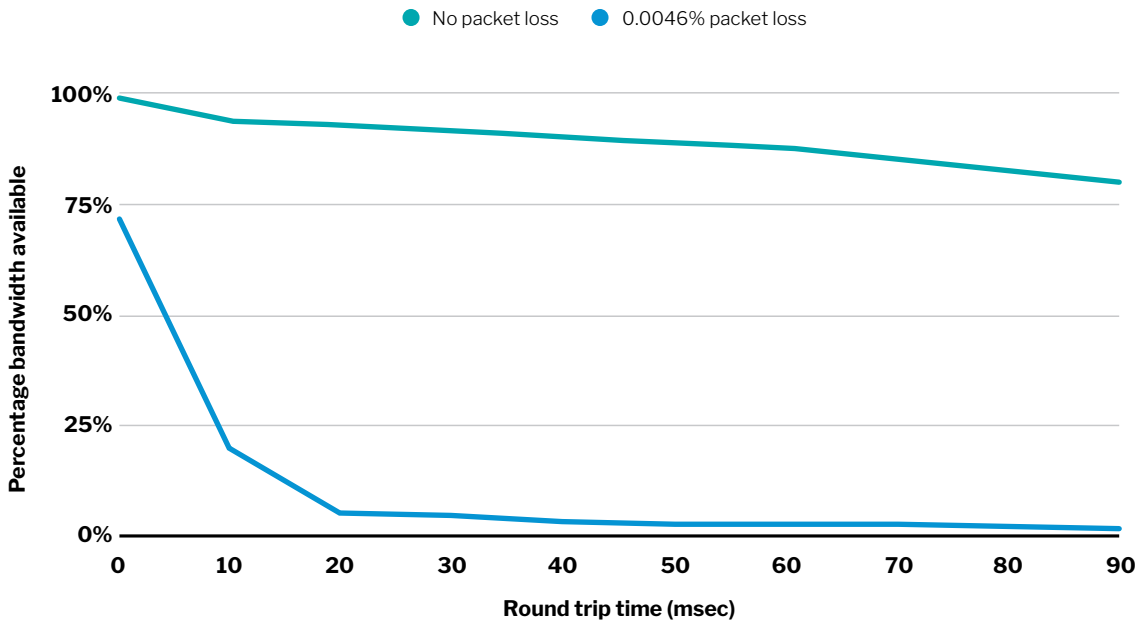
Say remote work security takes priority over performance

69.3%

Believe security negatively impacts performance and user experience

Latency and Packet Loss Impact on Throughput

Zero Packet Loss and 0.0046% Packet Loss



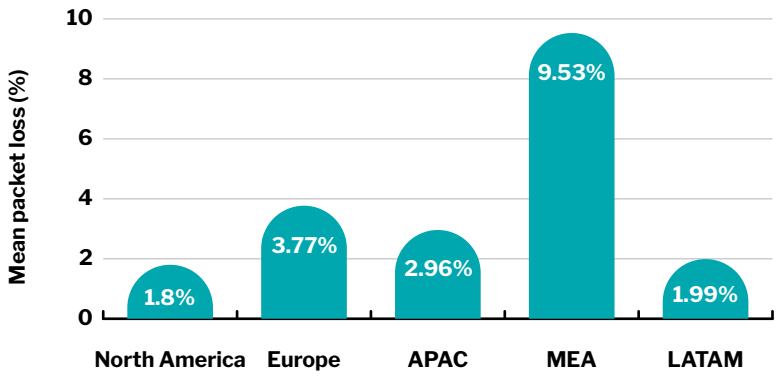
Less than .005% packet loss drops TCP throughput by 90%.

Measured throughput vs. latency on a 10Gps link with 0.0046% packet loss

Packet loss is more prevalent than expected

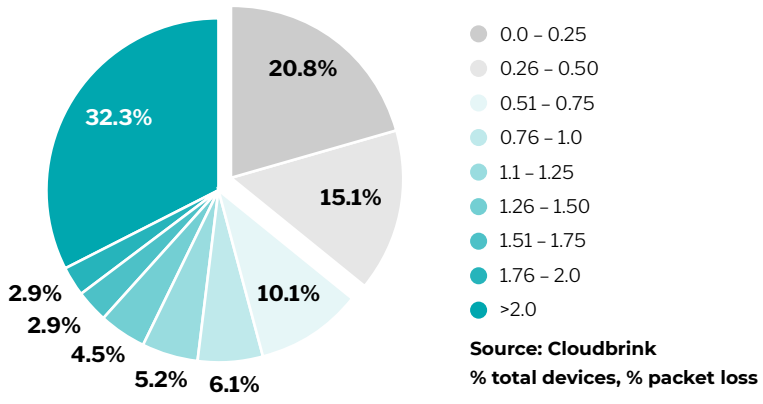
While remote and hybrid work notoriously experience significantly higher latency due to oversubscribed ISP networks and other factors, few experts understand the compounded impact of adding even miniscule amounts of packet loss. Cloudbrink data shows the sheer prevalence of packet loss exceeds expectations — even in the US.

Average Packet Loss By Global Region



Overall, 60% of end users struggle with packet loss above 0.5%, enough to greatly exacerbate the impact of normal network latency.

US Packet Loss Distribution



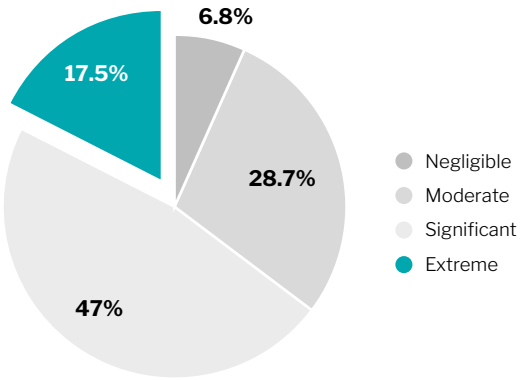
Source: Cloudbrink
% total devices, % packet loss

Less than 20% of respondents consider the significance of 0.5% packet loss to be extreme. This lack of understanding leads to bad investments and taking the wrong steps to fix performance problems.

Less than half (47%) of survey respondents expect a 0.5% packet loss to have a significant impact on application performance for remote workers and only 17.5% would expect an extreme impact — a gross underestimation.

Experts also may fail to grasp the extent to which mitigating the effect of packet loss would avoid the performance tradeoffs that come with stronger security.

Expected Impact of 0.5% Packet Loss



50.6%

Would most likely attempt to remediate remote access performance problems by upgrading user devices

41.8%

Would most likely upgrade or replace applications

Remote access solutions also drive cost and complexity

Over 70% of survey participants consider their current remote access solutions challenging and costly to roll out. Nearly 8 out of 10 (78.5%) also find them difficult to manage. With remote and hybrid work on the rise and technical resources challenged to keep pace, organizations need new solutions that generate less work and fewer support tickets.

53%

Consider their IT environments more complex than they were 2 years ago

40%

Cite remote and hybrid work as the most common reason for the added complexity

Source: ESG

Packet loss: The ten-ton gorilla lurking in the shadows

IT professionals know that network latency hinders performance by denying applications the full use of bandwidth, but grossly ***underestimate the impact of packet loss*** on the hybrid work experience. In wired networks, packet loss stems from congestion issues, hardware and software glitches, and over-subscription. Wireless networks face additional challenges from interference, signal-to-noise ratio (SNR), distance, and channel overload. Oversubscription on ISP networks also causes spikes that result in dropped packets.

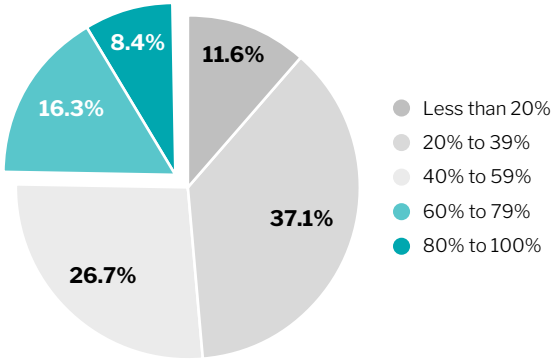
Too many retransmission attempts detract from the quality of streaming video, conferencing services, large file transfers and content downloads, and other processing- or data-intensive applications, especially as distance increases. Packet loss severely limits throughput and is particularly prevalent in the last mile — the part of the network that's beyond IT's control and where the majority of problems arise.

PART I.

REMOTE WORK IS NOW JUST WORK — ORGANIZATIONS SECURE ACCESS IN NEARLY EVERY WAY

Research by Upwork[1] shows 32.6 million Americans, or approximately 22% of the overall workforce will work remote by 2025. Our survey findings concur with nearly 1 in 4 organizations reporting that **60% or more of their employees work remotely at least 1 day per week.**

Employees Working Remotely At Least One Day Per Week



Companies use a variety of secure remote access technologies

Solutions for securing hybrid work range from traditional technologies like virtual private networks (VPNs) and virtual desktop infrastructure (VDI) to sophisticated modern frameworks like SASE and ZTNA. On the whole, responses show organizations evolving toward modern, comprehensive strategies to overcome the limitations of legacy approaches.

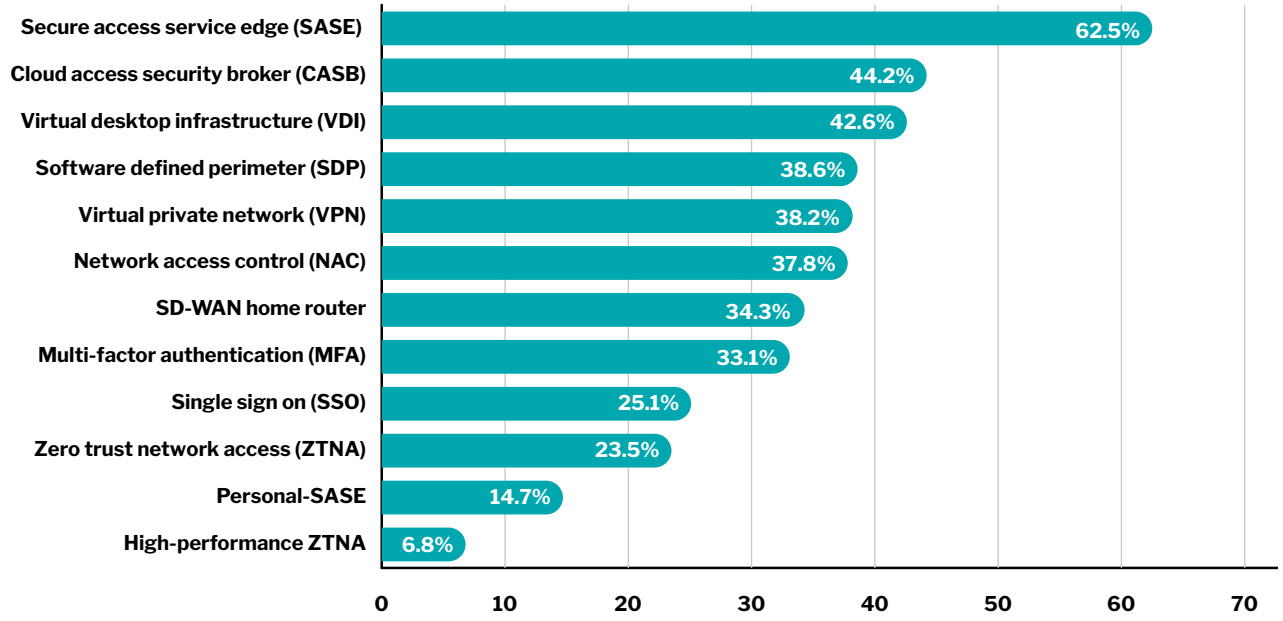
33.5%

Of respondents use SASE as their *primary* hybrid work access solution

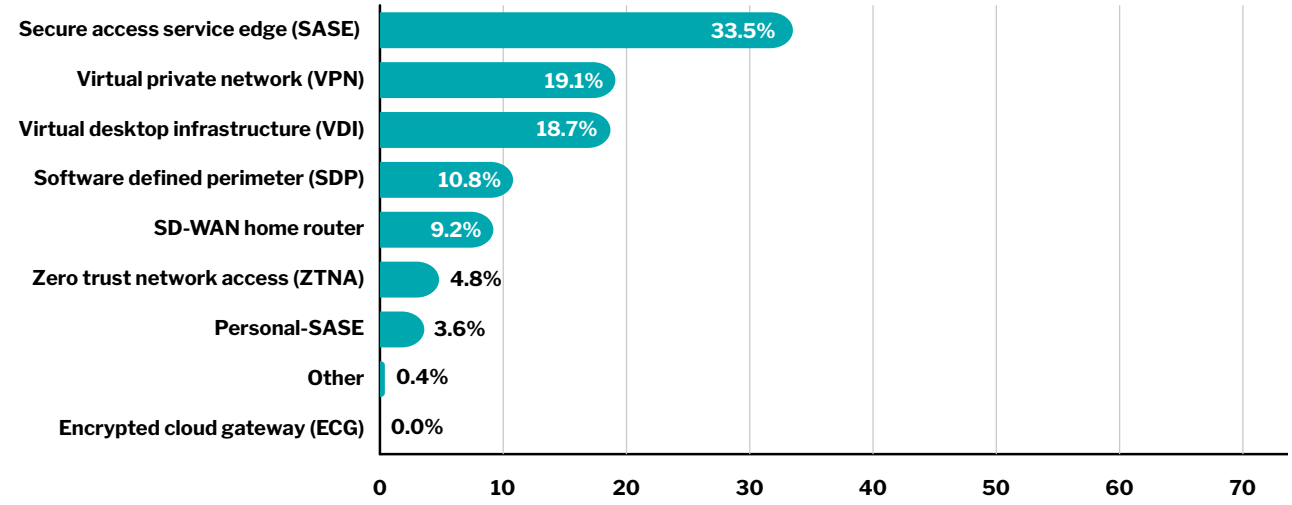
1. https://www.upwork.com/press/releases/upwork-study-finds-22-of-american-workforce-will-be-remote-by-2025#:~:text=By%202025%2C%2036.2%20million%20Americans%20will%20be%20remote%2C%20an%20increase%20of%2016.8%20million%20people%20from%20pre%2Dpandemic%20rates

The highest overall percentage of participants use SASE (62.5%) with more than a third using the approach as their organization's ***primary*** remote access solution, followed by traditional VPNs and VDI at just under 20% each. While few companies rely on ZTNA as their primary solution (4.8%), its adoption gets reflected in their choice of SASE that combines software-defined wide area networking (SD-WAN) and Zero Trust security principles.

Remote Access Solutions Currently in Use



Primary Remote Access Solution



Predictably, the highest adoption of SASE occurred within large organizations with 10K employees (50%) while the highest reported usage of VPNs (27.7%) was reported at smaller companies with less than 1K employees and presumably tighter resource constraints. With less effective approaches like VPNs still widely in use — even among security-conscious sectors like financial services and manufacturing — ample opportunity exists to evolve to more powerful and effective solutions.

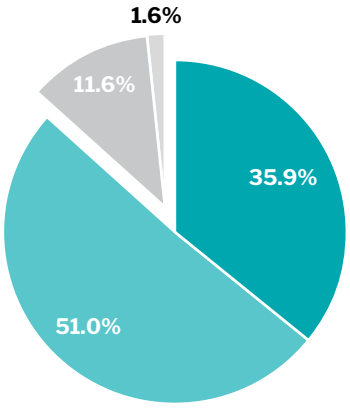
PART II.

SECURITY GETS SELECTED OVER PERFORMANCE, BUT WHAT IF YOU COULD HAVE BOTH?

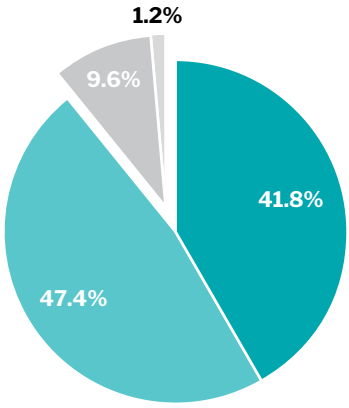
In a world where users, applications, and data all move with blazing-fast speed, businesses continue to emphasize security — regardless of its impact on performance. **Nearly 1 in 9 respondents (87%)** say having robust end-to-end security for remote access is their organizations' top priority even if it negatively impacts performance and user experience.

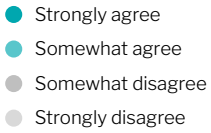
Consistent with this sentiment, participants believe the solutions their organizations have in place provide robust security for all business use cases. Respondents expressed higher overall satisfaction with the 'end-to-end security' (4.15 out of 5) achieved by their companies' remote work solutions compared with 'end-to-end performance' (3.94).

Security is Prioritized Over Performance



We Have Robust Security for All Use Cases



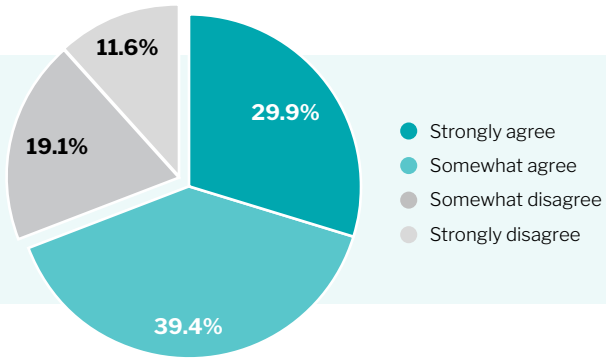


More than three-quarters (78.3%) of those surveyed understand that the security capabilities of their companies' remote access solutions negatively impact performance with nearly a third (29.9%) agreeing strongly. Yet companies know security that comes at the expense of performance cannot sustain growth long-term.

Legacy approaches result in lower user satisfaction

Significantly higher percentages of respondents whose companies use VPNs (75%) and VDI (74.5%) as their primary remote access solutions agree the security capabilities of their remote access solutions negatively impact user experience and performance compared with those who primarily leverage SASE (65.5%).

Security Negatively Impacts Performance

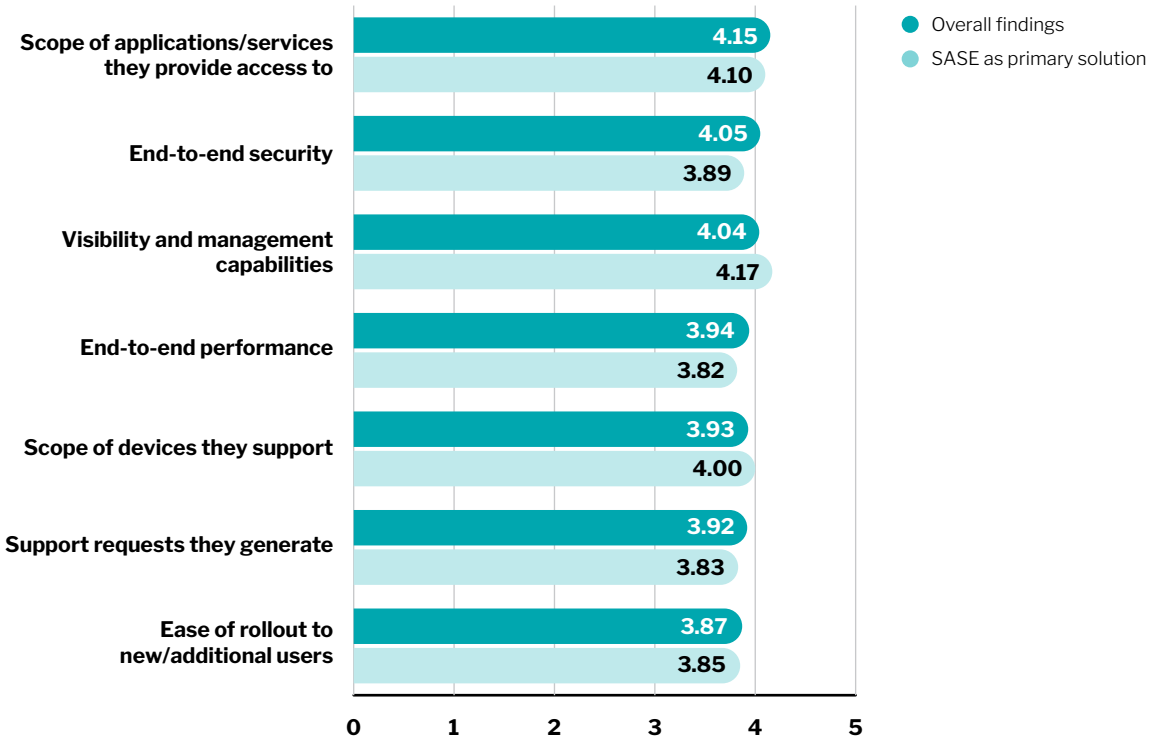


Three-quarters of respondents whose companies use VPNs (75%) and VDI (74.5%) as their primary remote access technology say security negatively impacts user experience

SASE can't fire a silver bullet

Those who identified SASE as their primary solution expressed below average satisfaction with end-to-end security as well as end-to-end performance. This finding potentially indicates these organizations have set the bar for security higher than others and possess greater awareness of the need to continually evolve their strategies and postures toward 'secure productivity.'

Satisfaction with Remote Access Capabilities

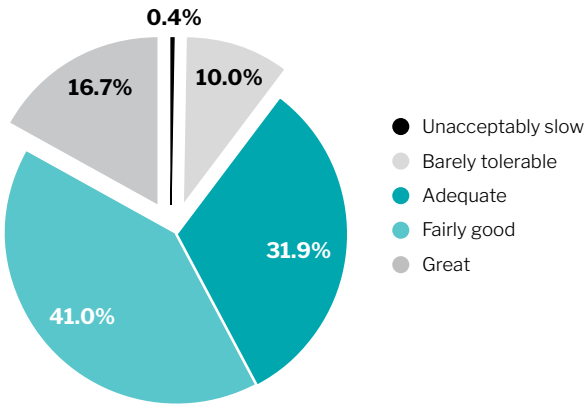


PART III.

PROBLEMS PERSIST AS TRADITIONAL SASE FAILS TO FIX PERFORMANCE ISSUES

On the whole, the IT and security professionals who participated in the survey categorize users' perceived experience with remote access solutions as adequate or fairly good (72.9%). Respondents at technology companies were most likely to rate user perceptions as 'fairly good' (48%) while those at finance companies — which tend to boast larger budgets — were twice as likely to rate user experience as 'great' (32%).

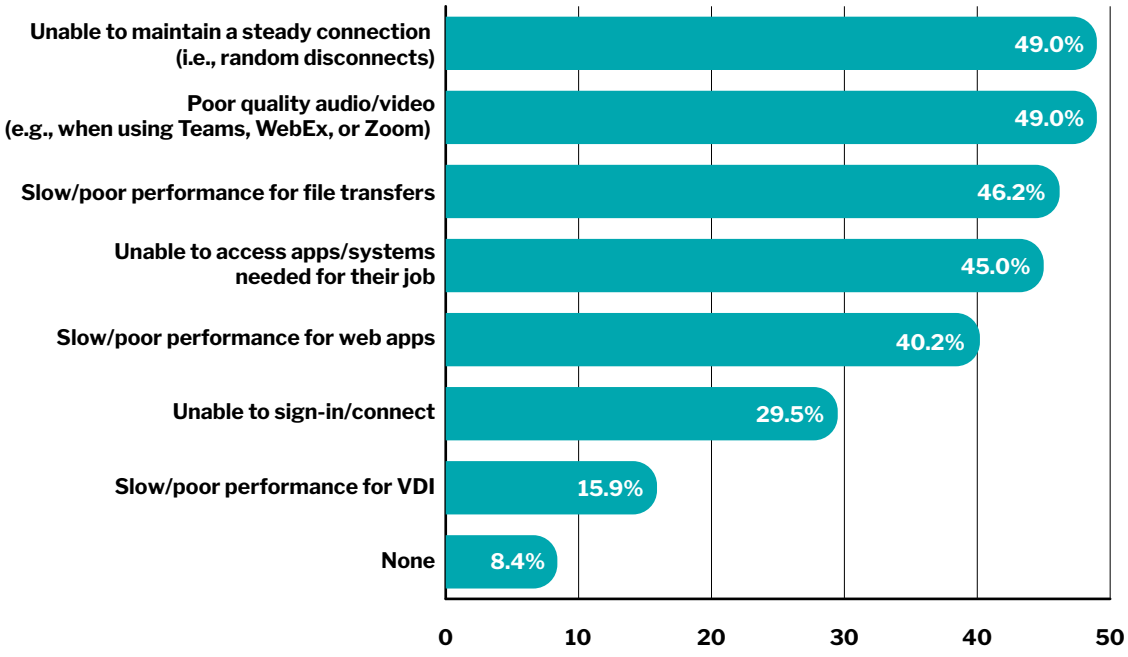
Remote Access Performance



Detractors to performance include connectivity and video quality

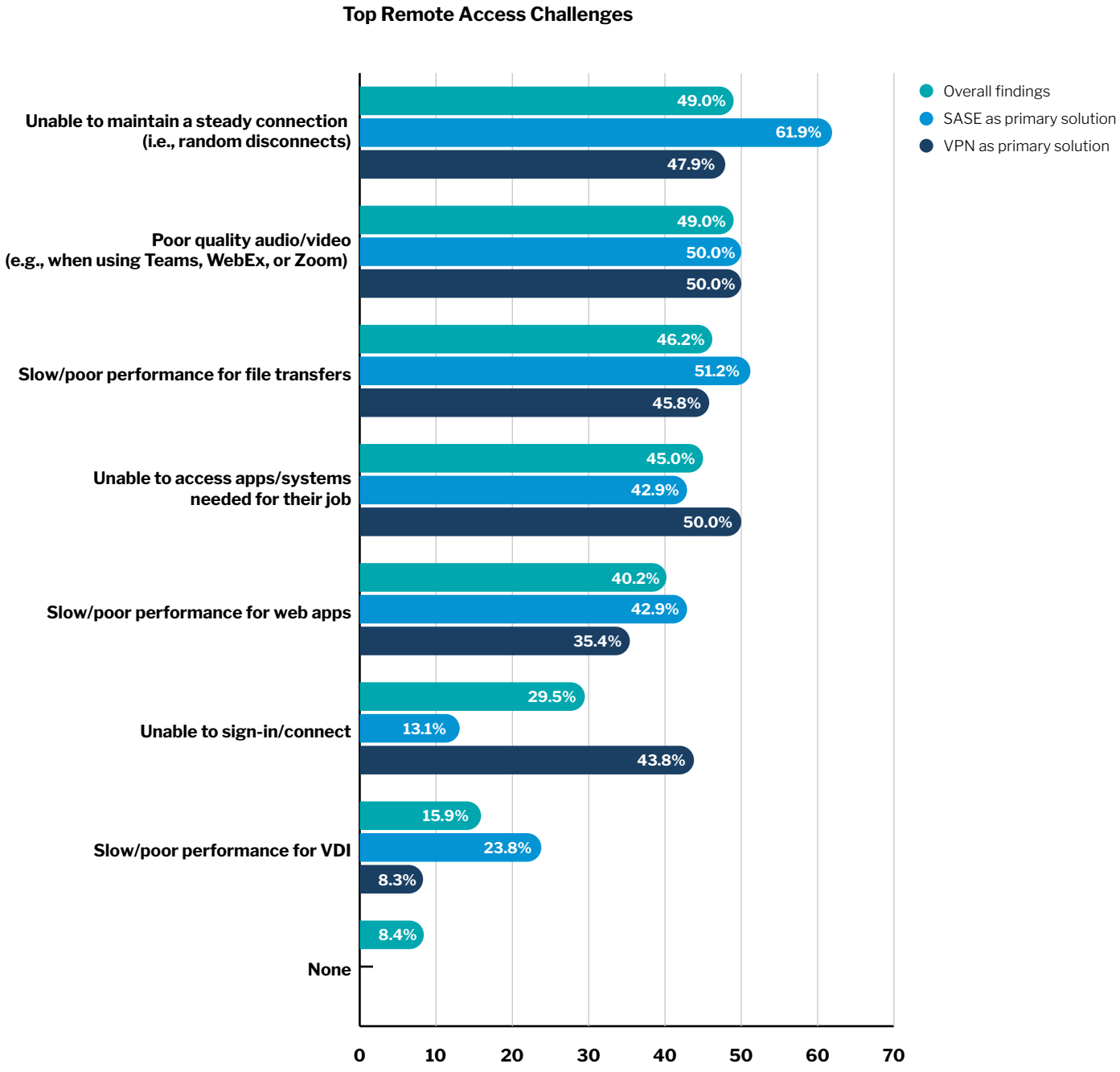
When asked about factors impacting remote and hybrid workers' satisfaction, user experience often suffers due to poor connectivity and sub-par experiences with conferencing/collaboration applications and file transfers.

Top Remote Access Challenges



Respondents less satisfied with SASE connectivity

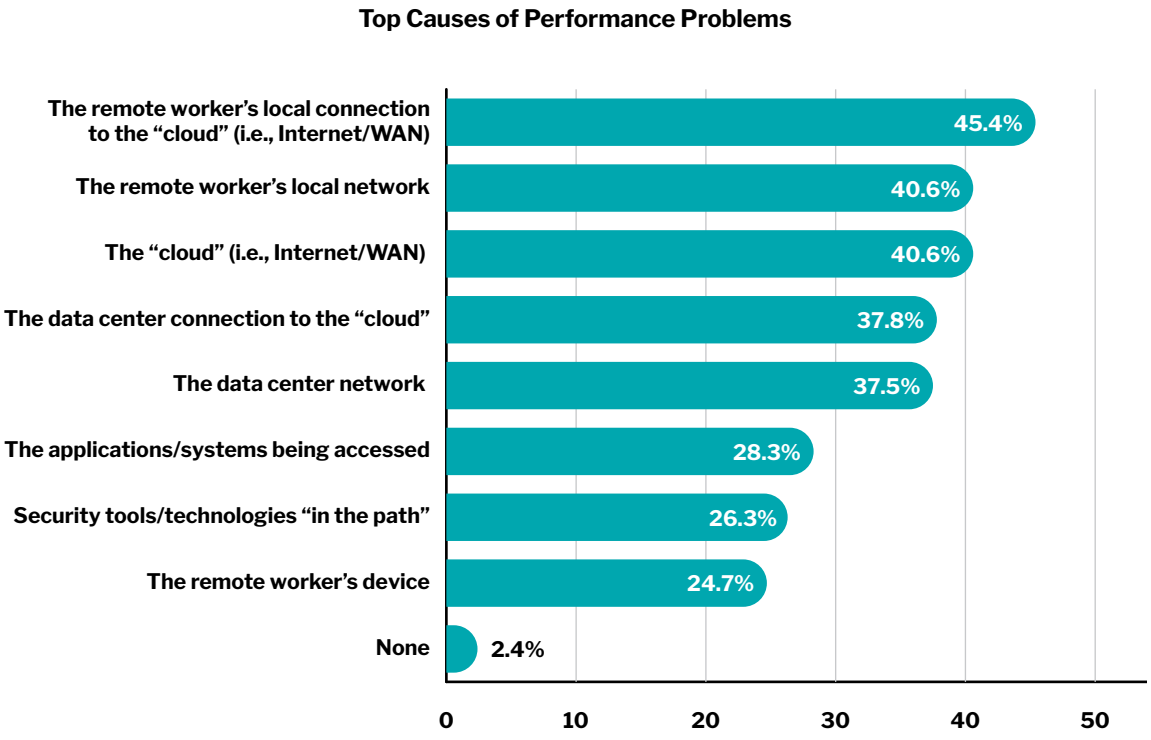
A significantly higher percentage of respondents whose companies rely on SASE as their primary remote access technology report difficulties maintaining a steady connection (62%) compared with those who rely primarily on VDI and VPNs (less than 50%).



Perhaps influenced by the likelihood of having to field user complaints, IT professionals were more than twice as likely as security professionals to emphasize user issues with signing in and connecting to company resources.

IT believes most problems occur beyond their control

According to IT and security executives, the top three causes of remote access performance issues revolve around networking and connectivity problems. Respondents rate remote workers' connections to the Internet and the performance of local and cloud networks more impactful than data center network and connectivity issues. They also deem connectivity more impactful than applications, devices, and security controls — three aspects within the direct purview of IT and security teams.



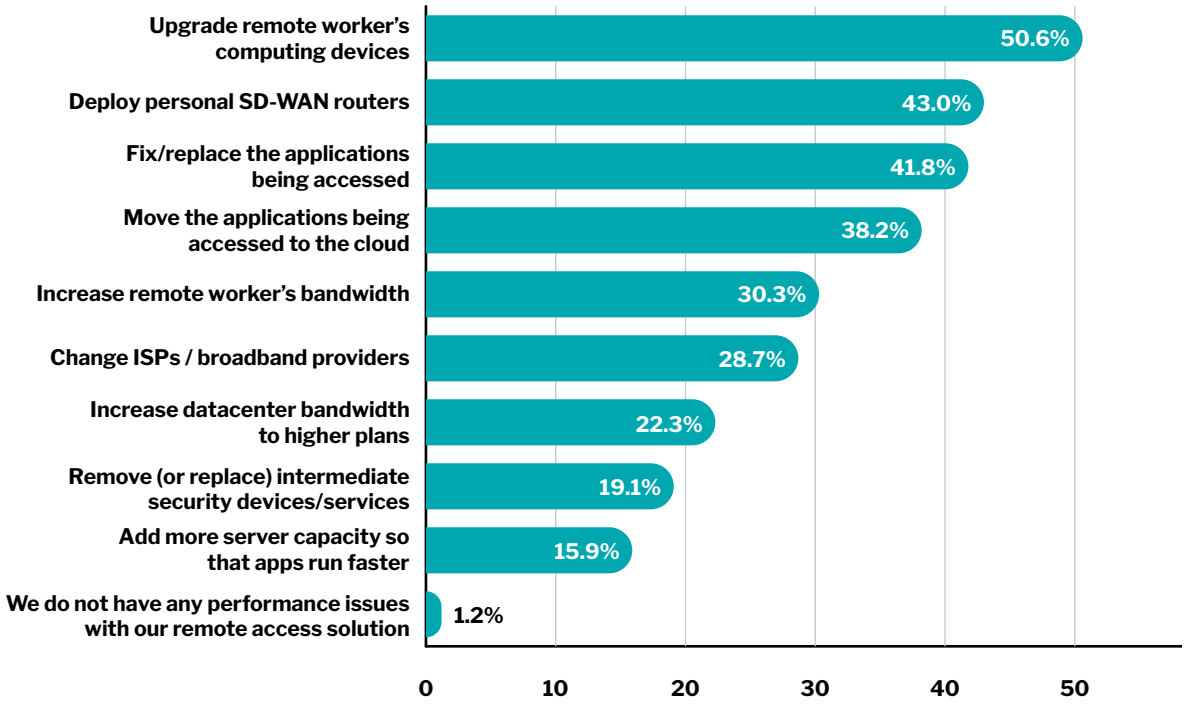
Respondents did not rank "security tools and technologies in the path" among the top contributors to performance problems. This suggests a clear lack of understanding of the combined impact of the latency added by security tools—and remote work in general—when combined with packet loss. Respondents from companies in the financial sector report the highest expectations for packet loss to have significant or extreme impact on performance at 79.1% while those at technology companies were surprisingly less likely to predict an extreme impact at 20%.

Go-to fixes don't resolve the source of problems

While networks and connections ranked highest on IT professionals list of factors contributing to poor experience, two of the three leading fixes IT applies do not address these issues head-on. Two of the reported top three — upgrading user devices and fixing or replacing applications — do not resolve connectivity challenges they say cause the most problems.

The disconnect between the perceived sources of performance problems and the actions IT teams say they're most likely to take points to massive investment in fixing the wrong things — or fixing the right things in the wrong ways.

Top "Fixes" for Remote Access Performance Issues



Limited visibility breeds limited understanding

Only 19% say they have end-to-end visibility of remote access performance while another 30% can only diagnose the root cause of issues 50% of the time or less. Low visibility and control over networks and connectivity issues leads to a shotgun approach to resolving user issues.

PART IV.

BUSINESSES PLAN TO INVEST, BUT TRADITIONAL APPROACHES DON'T DELIVER

Nine out of 10 respondents say their companies plan to invest in improving secure remote access

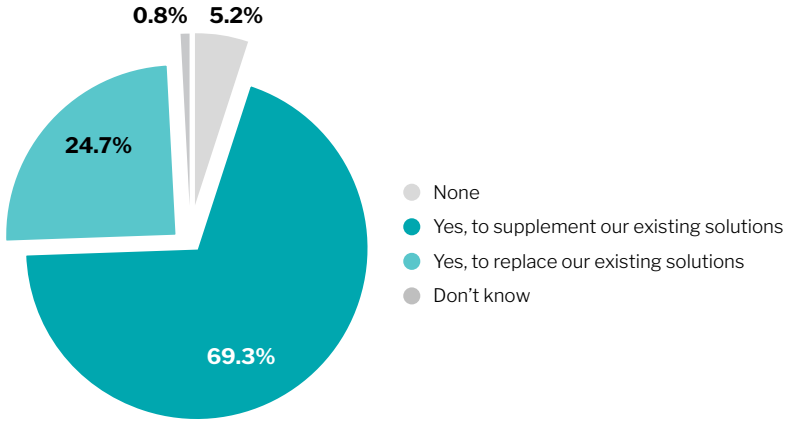
Virtually all participants' companies plan to upgrade or replace their current remote work solutions with 1 out of 4 projecting a complete swap out. Significantly higher percentages of both security (48.1%) and IT (35.7%) ***architects*** — the professionals likely to be involved in designing new solutions — plan to swap out existing technologies completely.

Predictably, larger organizations also report above-average intent to swap out solutions completely at 35.7%.

28.6%

Of organizations with traditional SASE as their primary remote access solution plan to swap out their current solution within the next 12 months.

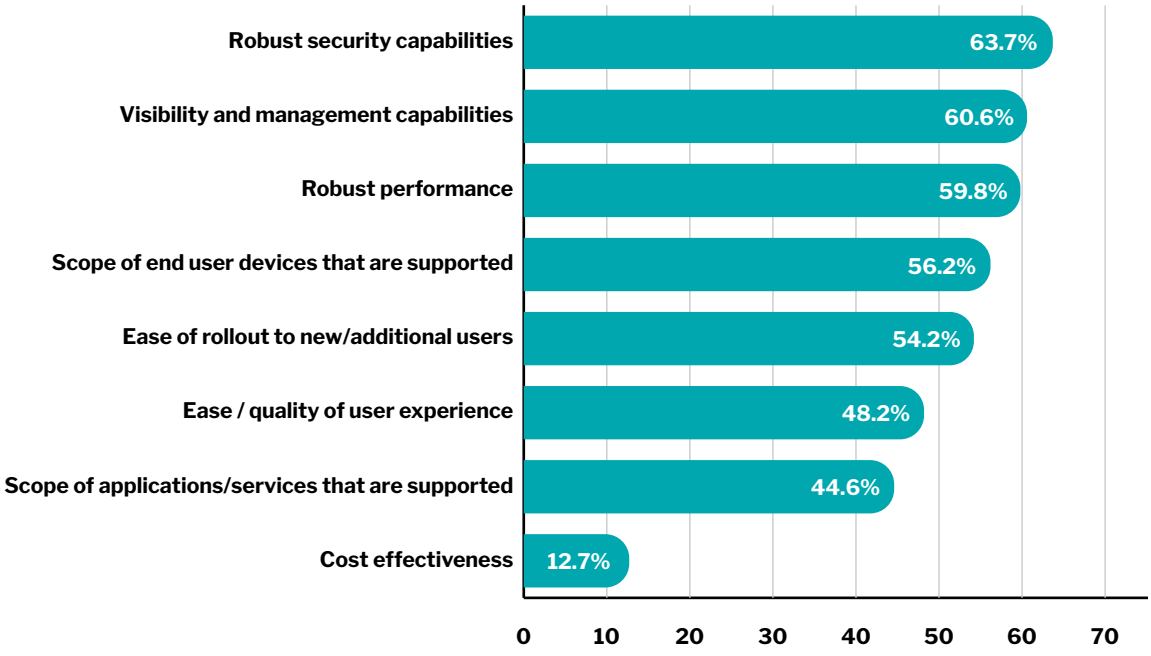
Plans to Invest in Remote Access Solutions



Solutions must balance security with performance

While 'robust security capabilities' still tops respondents' list of desired capabilities and characteristics for a new solution at 63.7%, 'robust performance' ranks only slightly lower at 59.8% (and third overall). More than 75% of IT managers emphasize strong security compared with 63.7% overall.

Top Capabilities/Characteristics for Secure Remote Access Solutions



Innovations should address complexity

In a recent study by Enterprise Strategy Group (ESG), more than half (53%) of respondents deemed their IT environments more complex now than they were two years ago, due in part to the growth of remote and hybrid work. In response, nearly a third of those participating in the survey plan to invest to improve connectivity to deliver a better user experience.

Visibility and control remain strong considerations — second in priority overall — as companies consider potential remote access solutions. The fact that respondents assign high value to being able to see, control, and manage secure remote access likely comes as a reaction to their current experience with legacy solutions.

One Cloudbrink customer was able to migrate

100%

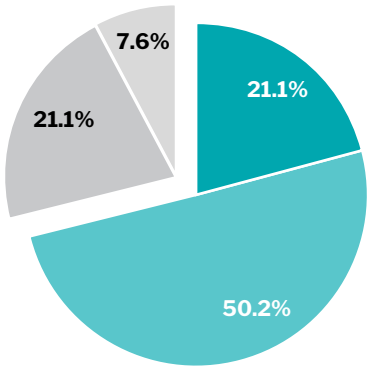
Of its workforce to Personal SASE and redeploy

50+%

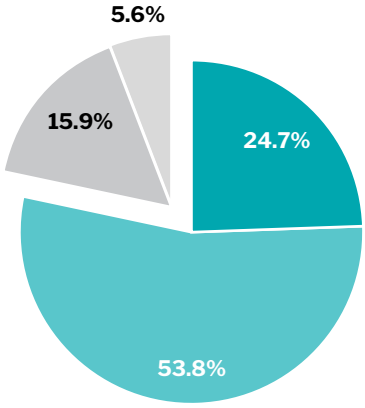
Of its supporting technicians to strategic security initiatives within

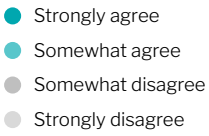
3 Weeks

Remote Access is Cumbersome/Costly to Rollout



Maintenance/Support is Onerous





The vast majority of participants (71.3%) agree their current solutions prove cumbersome and/or costly to roll out. An even larger percentage (78.5%) say ongoing management takes considerable effort with 1 in 4 agreeing strongly with this idea.

New strategies offset packet loss and meet goals for user experience and ROI

IT teams employ a proven but costly fix for handling poor performance — they simply add bandwidth — but overinvesting to overprovision won't lessen the impact of packet loss compounded by latency. While they can't control or eliminate the problem, companies can apply new techniques to offset its impact on performance.

Due in large part to packet loss, even mature security frameworks such as SASE and ZTNA have yet to deliver satisfactory performance, security, and ease of use at the same time. Rather than move from one unwieldy — and underwhelming — solution to another, innovative techniques may be used to overcome challenges inherent in modern remote access frameworks.

Cloudbrink's innovative **Personal SASE** with **High-performance ZTNA** empowers the **"work-from-anywhere"** generation with secure, adaptable networking. This industry-first solution integrates ZTNA to centralize visibility, streamline security, and deliver unparalleled performance and low-latency access from any location.

For acceptable performance the user's network should have packet loss below

0.005%

but the average in the US is 1.8%. Cloudbrink recommends Personal SASE to overcome packet loss as high as 10%.

Leading options to balance hybrid work security and performance

Zero Trust Network Access (ZTNA) security services verify user identity before granting access to applications. In contrast with VPNs, ZTNA denies access to applications and data by default and only grants access those requested.

Secure Access Service Edge (SASE) framework combine software-defined wide area networking (SD-WAN), ZTNA and cloud access security brokers (CASB) into a secure, cloud-based connectivity platform.

Cloudbrink Personal SASE aims to overcome the complexities of deploying traditional SASE to replicate the seamless in-office user experience in external settings without compromising security. Cloudbrink's service addresses latency and packet loss by leveraging FAST edges to preempt and accelerate packet recovery. The Cloudbrink protocol carries context and makes per-hop decisions to optimize performance and recover lost packets without disrupting end-to-end encryption.

How much does packet loss cost you? Find out now.

One Cloudbrink user calculated the annual cost of users wasting time as they waited for files to download and large data transfers to complete at roughly ***$3K per user per year***.

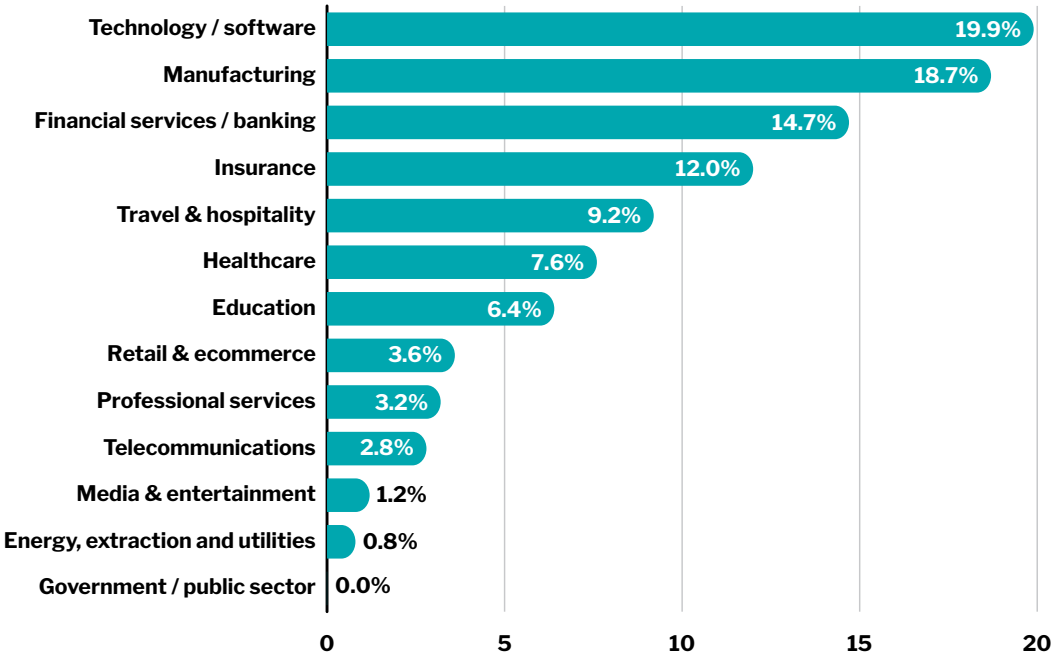
Download the free packet loss tool to help identify bottlenecks impacting your organization.

APPENDIX

Survey Demographics

In addition to Cloudbrink data from hybrid workers, the company commissioned a research firm to poll IT and security professionals from more than 250 enterprises from a diverse array of industries. The respondent breakdown is as follows:

Survey Participants by Industry



Survey Participants by Role

27.1%
CIO, CTO, or VP of IT

19.5%
IT director, manager, or team lead

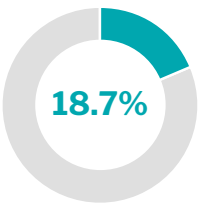
18.7%
CISO, VP of IT security, or IT security executive

12.7%
IT security director, manager, or team lead

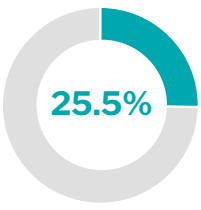
11.2%
IT architect or engineer

10.8%
IT security architect or engineer

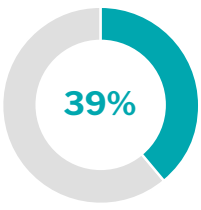
Survey Participants by Size of Organization



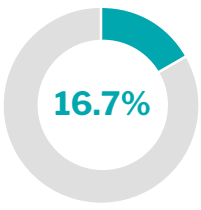
500-999



1,000 - 4,999



5,000 - 9,999



10,000+