REPORT

A10 Networks International Communications Service Providers Insights 2021

This research analyses how senior IT professionals in communications service provider organisations will adapt to a post-COVID-19 world, and the challenges they face with a more distributed workplace.

TABLE OF CONTENTS

INTRODUCTION

This research was conducted to understand the challenges and issues facing communications service providers when it comes to the lasting impact that COVID-19 has had on their subscribers and enterprises. It identifies trends in demand and usage patterns, expectations around security and resiliency in what has been an unprecedented year. It examines communications service providers' plans for investment, adoption of new technologies, and the complexity of operating in the current hybrid environment

Read this analysis to discover how senior IT professionals in communications service providers are planning to adapt to the new post-pandemic world and the challenges they face with a more distributed workplace.

Methodology

A10 Networks commissioned a survey, undertaken by an independent research organisation, Opinion Matters, in January 2021. 1251 senior IT professionals from a range of communications service providers were surveyed including: mobile, fixed-line telecom, cable, converged, MVNO and MVNA and OTT providers.

Additionally, the research was undertaken across five countries, including: UK, France, Germany, Middle East and India.

FOREWORD – INSIGHTS INTO THE INTERNATIONAL COMMUNICATIONS SERVICE PROVIDERS LANDSCAPE

Without a doubt, the pandemic has had a lasting effect on all businesses during 2020. In particular, it has impacted communications service providers who overnight experienced a massive change in usage patterns with the huge shift to remote working. Operators had to respond very quickly to this rapidly changing demand – both in terms of the surge in requirements and the broader locations they now need to serve.

To this point, nearly all the respondents **(99%)** from our research stated that they **had experienced an increase in demand as a result of COVID-19** and this has led to a huge scale up of their infrastructure, networks and technologies.

Clearly, a return to pre-pandemic working practices is unlikely to happen and a large proportion of the senior IT professionals that we surveyed were adamant that the workplace won't snap back to how it was before COVID-19, and that they expect and are preparing for a hybrid approach to working practices.

The pandemic significantly raised awareness around the resilience of the network and the robustness of security, and going forward, subscribers and enterprises expect much stronger security from their communications service providers and will demand more in their SLAs and expand to other types of service providers to get this commitment.

We recently worked with telco analyst firm, HardenStance, which undertook a study on 'real world' cybersecurity incidents experienced by telco providers, and this highlighted just how vulnerable telcos and their customers are to a wide variety of threats including DDoS and ransomware, as well as attacks that exploit vulnerabilities in APIs and web servers.

This again was underpinned by our research whereby just under half (48%) of the surveyed providers stated that upgrading firewalls and other security appliances to meet new threats and increased traffic volume was their highest priority security investment in the next two years.

The research also highlighted the extent to which communications service providers are concerned about DDoS attacks and the need to mitigate them. Overall, it underlined that many communications service providers are vulnerable and, as a result of COVID-19, more are now investing in security in order to reinforce their defences.

Clearly, as communications service providers evolve with digital transformation and a cloud-native deployment model, they should prioritise applying more rigour to their security strategy — with up-to-date thinking and techniques — to address long-standing vulnerabilities.

TOP FINDINGS

A Distributed Environment is Leading to a Bigger and Broader Attack Surface

99% of all respondents said that COVID-19 had accelerated network plans to transition to a more distributed environment and affected more than a quarter of their traffic. They are seeing increased demand from different locations, and this has forced communications service providers to redistribute network capacity, to scale up in specific locations (54%) and increase headcount (32%).

47% have invested heavily in security technology as a result and 55% say that, going forward, better network security is required to deal with this distributed environment. And just under half (48%) of providers stated that upgrading firewalls and other security appliances to meet new threats and increased traffic volume was their highest priority security investment in the next two years.

The Impact COVID-19 has had on Relationships and Investment Plans

It is a mixed bag when it comes to investment. Some investment plans have been accelerated, particularly around security (52%), others are investing less in their own network and moving to invest more in public clouds (50%), while others have put their investment plans on hold (49%).

Where customer relationships are concerned, 56% have seen an increase in demand from customers for online platforms and portals so that customers/subscribers can self-serve. More than half (52%) are seeing customers nervous about the resilience of their communications service providers and are finding they are asking questions around business continuity. A significant number (44%) believe that customers and subscribers have increased their expectations for network security as a result of the pandemic.

Going forward, providers are keen to minimise or eliminate service interruption and downtime. Nearly all are planning multiple high-priority security investments including upgrading firewalls and security appliances (48%), adding DDoS protection services for enterprise customers (43%) and DDoS mitigation across the infrastructure (45%).

Without a Doubt COVID-19 had a Significant Impact

99% OF ALL RESPONDENTS

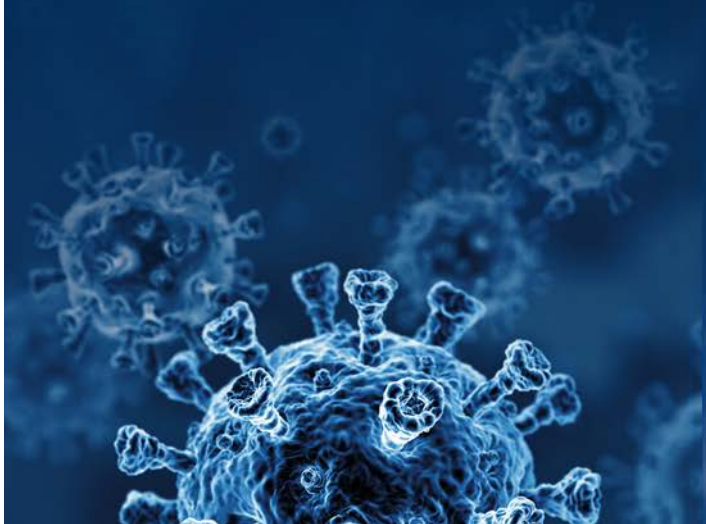
Experienced an increase in demand as a result of COVID-19 – on average by 55%

This resulted in communications service providers having to scale up in terms of:

Infrastructure across the network » **55%**

In specific high-demand locations » **54%**

Investing more heavily in security » **47%**



The Workplace Won't Snap Back to How it Was

67% believe their customers will continue to operate with employees working from home even post-pandemic. Only one-third (33%) believe the workplace will snap back to pre-COVID-19 working practices.

Enterprise Customers Face Additional Security Challenges

This hybrid workplace presents security challenges with 55% of respondents saying enterprise customers will have a requirement for better endpoint security to protect against increasing cyber-attacks. Companies need to get the basics right by having good endpoint security because organisations will only be as secure as the home networks they are on.

At the same time, communications service providers said that more than half of their enterprise customers are looking to revise their employee cybersecurity training programmes to reflect the hybrid work environment, and 47% stated that their customers will need to roll out multi-factor authentication to their workforce to enhance security. 42% say enterprises need to update their BYOD policies.

A Move to Less Traditional Non-Telco Providers

This has prompted a number of changes in the purchasing strategies of their enterprise customers, indicating that customers are exploring multiple approaches to increase resiliency. 58% say enterprise customers are splitting workloads and traffic between traditional telcos and non-telco cloud platform providers to ensure resiliency.

More than half (50.5%) are seeing customers requiring end-to-end security SLAs in order to protect themselves. 50% stated that customers have expanded their telco vendor RFP list to include non-telco cloud platform providers.

Concerns Around 5G and Multi-cloud Environments

When it comes to the diversity of environments with multi-cloud and 5G, providers are concerned that they can continue to deliver a good level of service, so outages are top of mind (47.5%), followed by compliance and regulatory requirements (43.5%) whilst also maintaining a consistent service for their subscribers (41%).

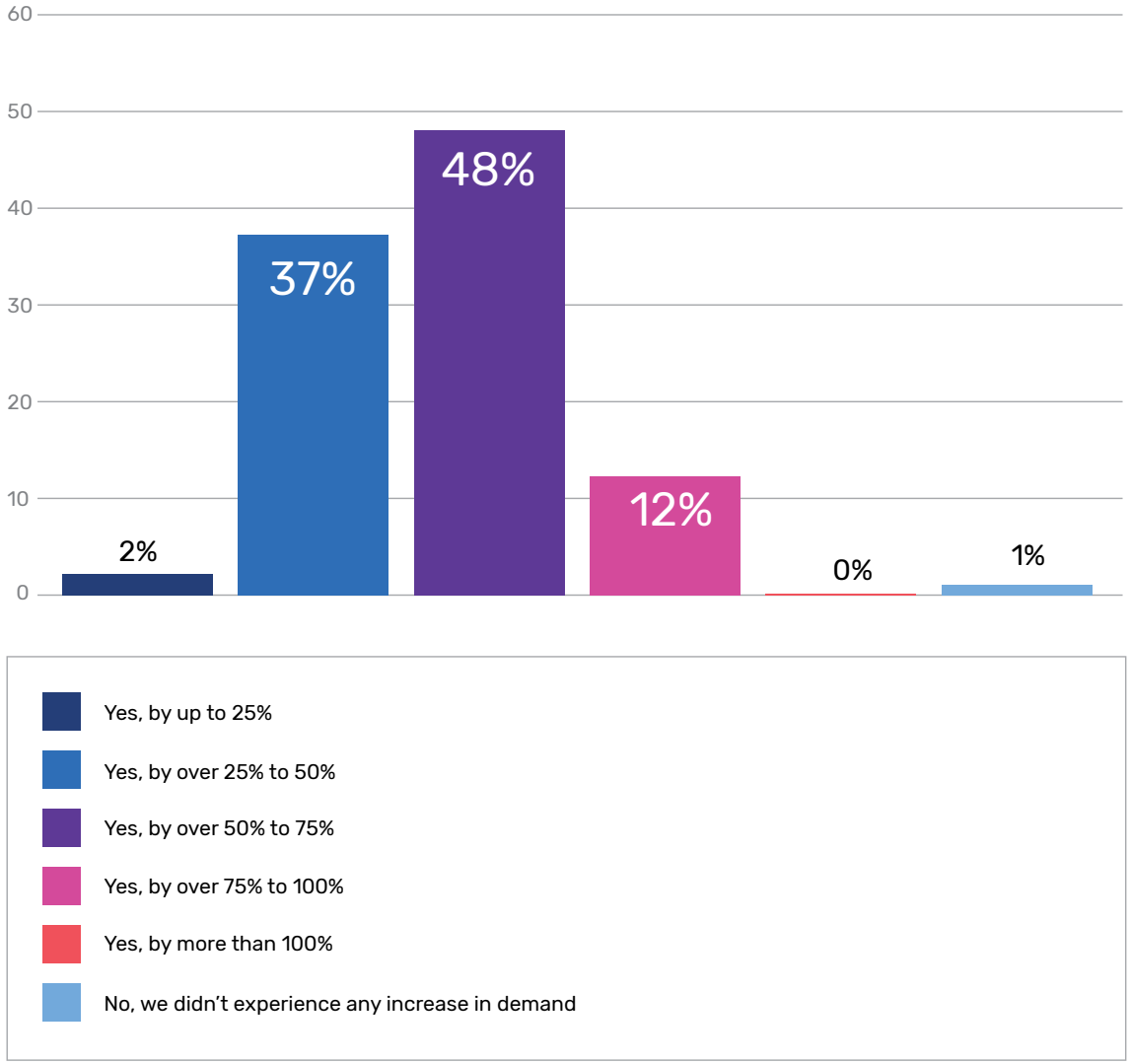
DDoS Protection is Finally a Key Initiative

DDoS protection is definitely a focus in the growing threat environment with 45% of respondents stating that DDoS mitigation across network infrastructure is a top priority security investment, while 43% said DDoS protection as a service for enterprise customers is the most important investment they planned to make.

And as the 5G network becomes more distributed, one-fifth said that growing threats of DDoS attacks on their distributed network architecture are a top security challenge. When asked about the additional capabilities and technologies communications service providers will need in 2021-22 to better protect customers and subscribers, granular customer-level DDoS mitigation came out on top with 45%.

FULL SURVEY RESULTS

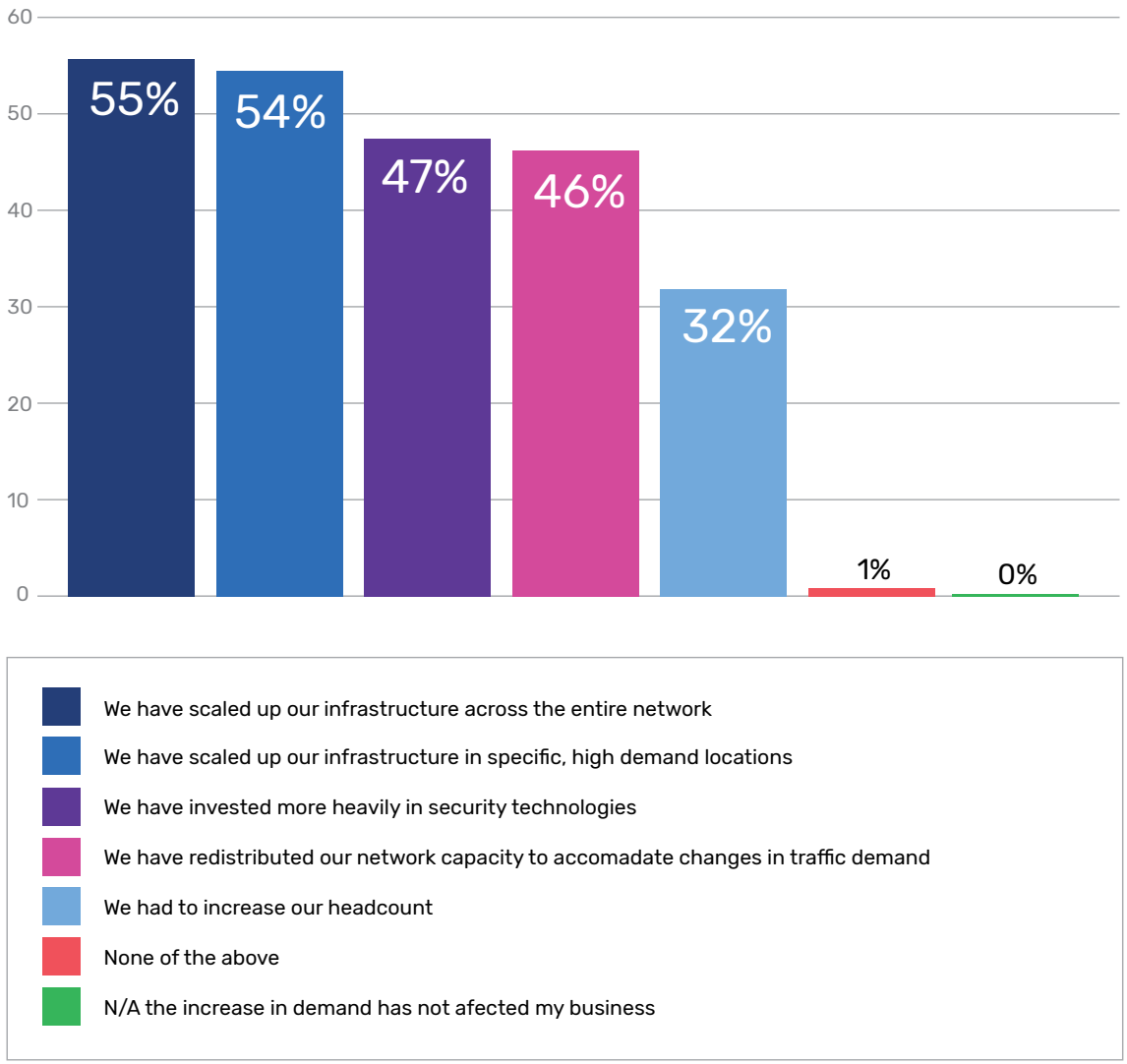
Did you experience increased demand for data and network bandwidth from your customers/subscribers as a result of COVID-19 and if so by how much?



Almost universally (99%) of respondents experienced an increase in demand for data and network bandwidth from their customers and subscribers, on average by 55%. This was clearly due to the rapid switch to remote working and then the continued lockdowns across countries and regions throughout the remainder of the year. 48% witnessed an increase in demand of over 50% to 75% and a staggering 12% saw an increase of over 75% to 100%.

The top-three verticals to see spikes in the over 75% and up to 100% category were gaming (13%) utilities (12%) and ecommerce and retail (11.5%).

Which of the following, if any, best describes how that increase in demand most affected your business?



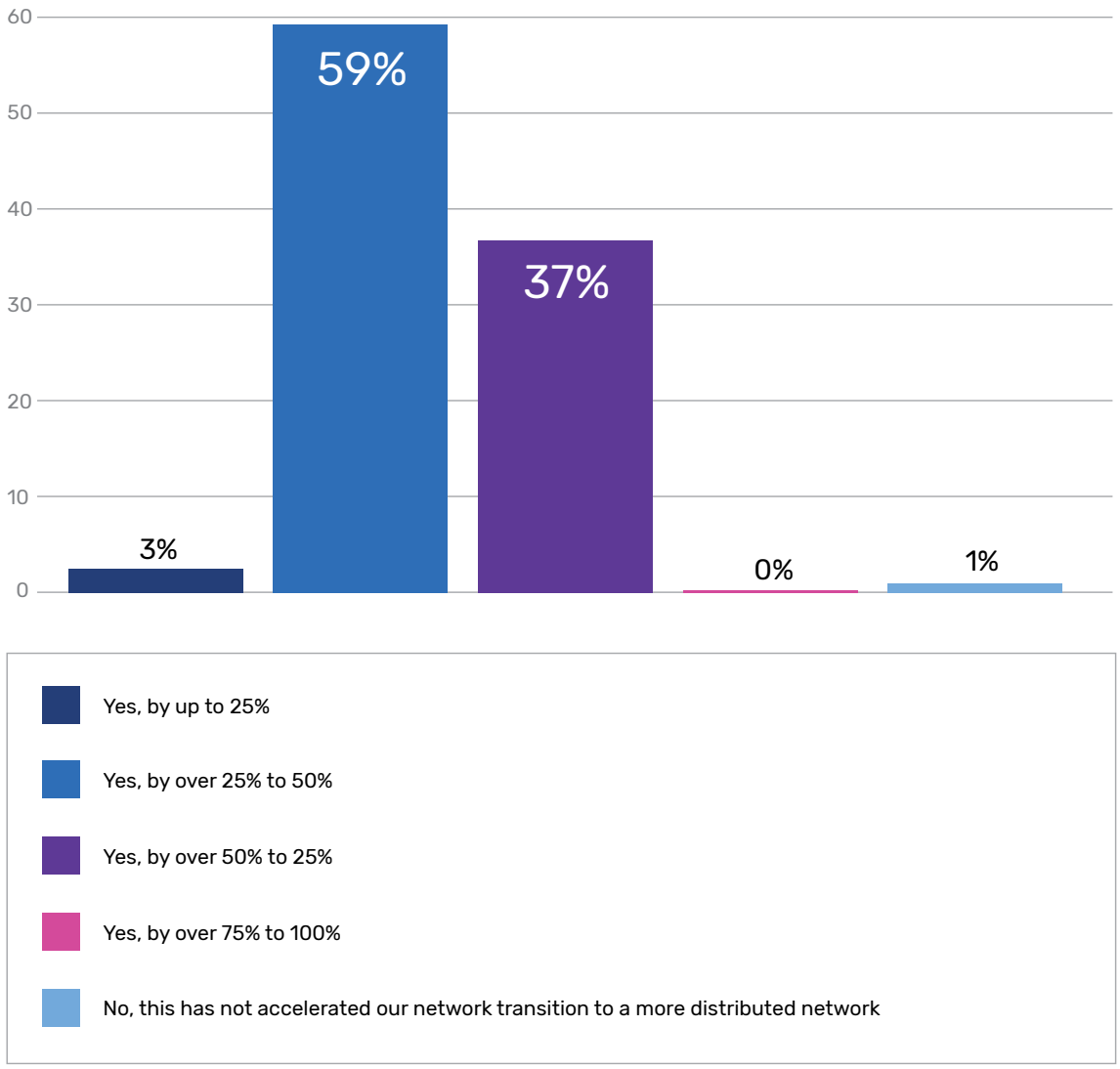
The top-three consequences of the increased demand were more than half (55%) stating that they had to scale up infrastructure across their entire network, 54% had to scale up in specific high-demand locations and 47% invested heavily in security technology.

Clearly the rapid surge in demand, owing to COVID-19, meant that communications service providers had to quickly expand their capabilities. But as organisations have moved to a remote set-up, so the attack surface has expanded and intensified, and this meant that respondents had to invest heavily in security technology to protect their networks. Likewise, demand has come from multiple different locations, whereby previously customers/subscribers were more likely to be in offices together, now workforces are geographically dispersed creating spikes in specific locations.

Other consequences have included a redistribution of network capacity to deal with varying demands and nearly a third (32%) have had to increase headcount to deal with this rise in requirements.

Respondents with customers in the education sector reported the highest in scaling up their infrastructure to meet specific high demand locations.

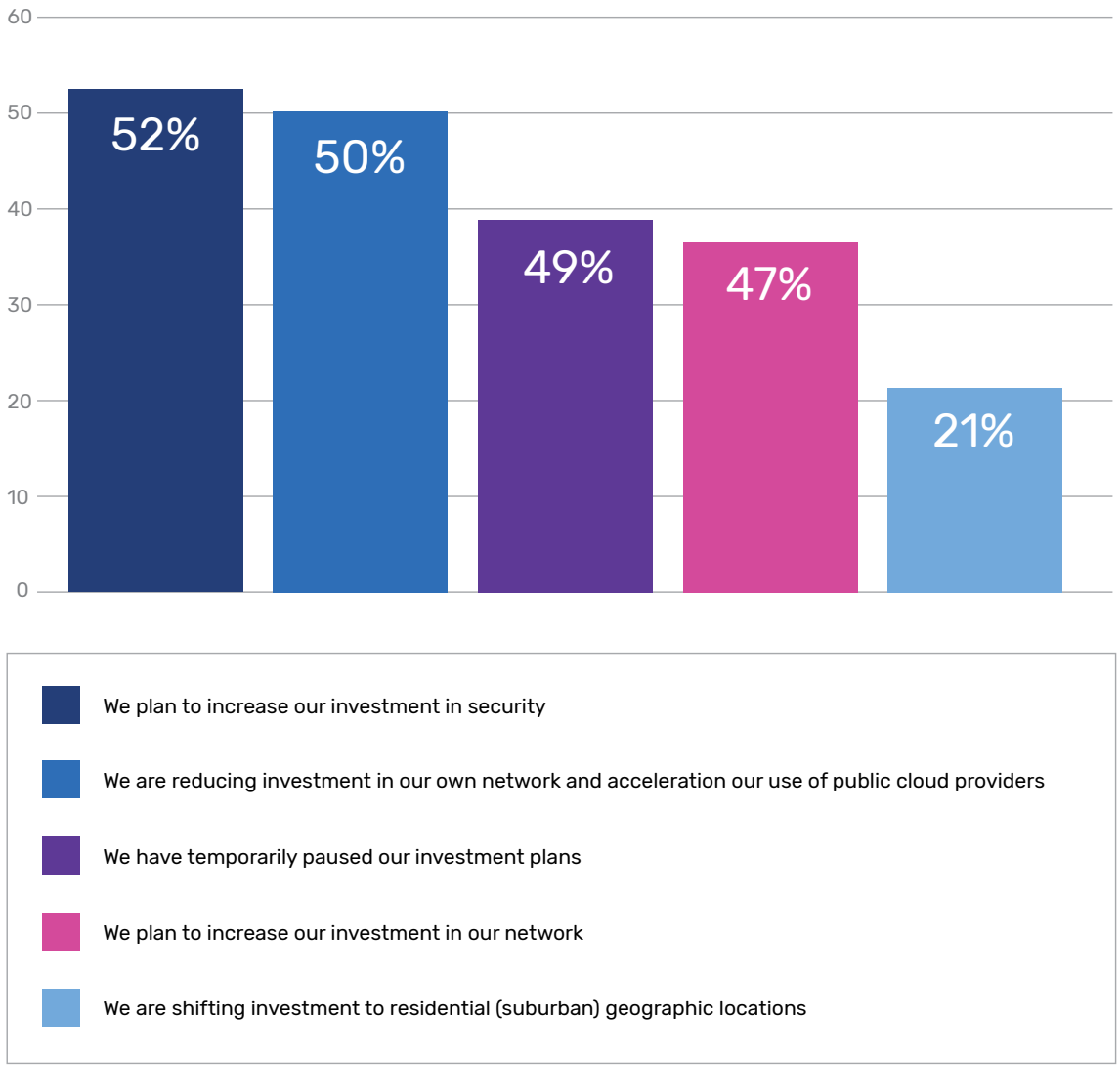
Has COVID-19 accelerated your network transition to a more distributed network (Edge) and how much of your total network traffic will this impact?



Overall, 99% of communications service providers stated that a transition to a more distributed network was accelerated by COVID-19, with more than half (59%) stating this impacted total network traffic by over 25-50%. Additionally, more than a third (37%) stated the impact was more than 50-75%.

Respondents serving the healthcare and utilities sector witnessed above average acceleration to a more distributed network by 66% and 67%, respectively, in the 25-50% category. While respondents serving the gaming sector were highest (38%) in the by over 50-75% category.

How, if at all, has this increase in traffic/subscribers changed your capital investment plans for the next 3 years?

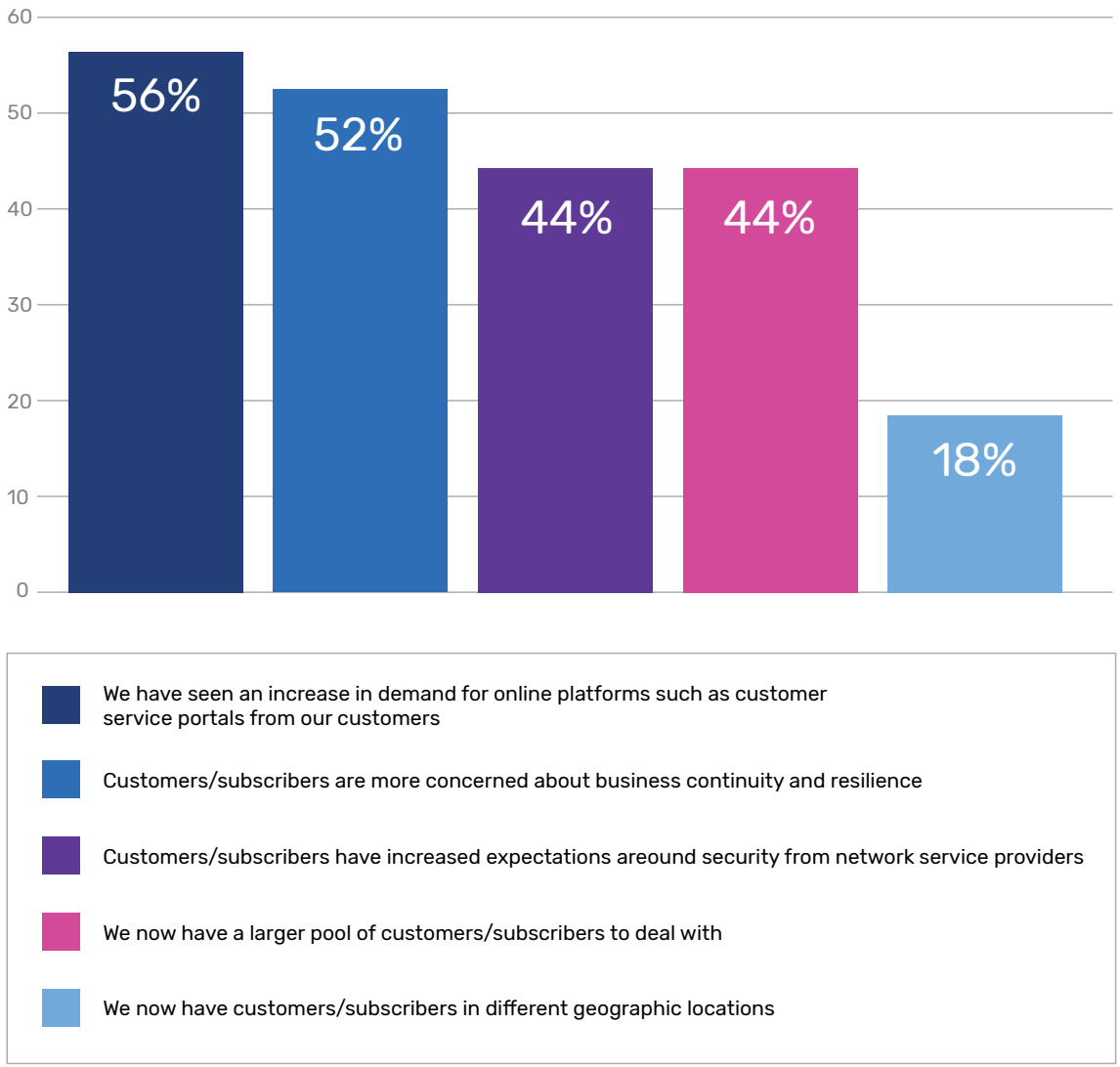


The increase in traffic has significantly changed capital investment plans for communications service providers in multiple ways. More than half of the respondents (52%) plan to increase their investment in security. Half of those surveyed (50%) are reducing investment in their own network and accelerating the use of public cloud providers, while 47% stated they plan to increase investment in their networks.

This increased investment in public cloud providers is likely due to heightened demand as organisations look to restructure their businesses and continue to work remotely following the pandemic. As companies work to recover, ever cautious about the economic impact from the pandemic, they will focus on creating a robust environment capable of dealing with future business interruption. However, just under half (49%) of respondents stated that they have paused their investment plans.

The smaller providers (250-499) are most likely to reduce investment in their own networks and move towards public cloud providers. Half of smaller providers were also looking to pause their investment plans (50.5%). Providers serving the healthcare sector were the highest in investing in security (60%) while 54% of respondents serving the government sector and 52% of respondents serving the education sector said they were pausing their investment plans.

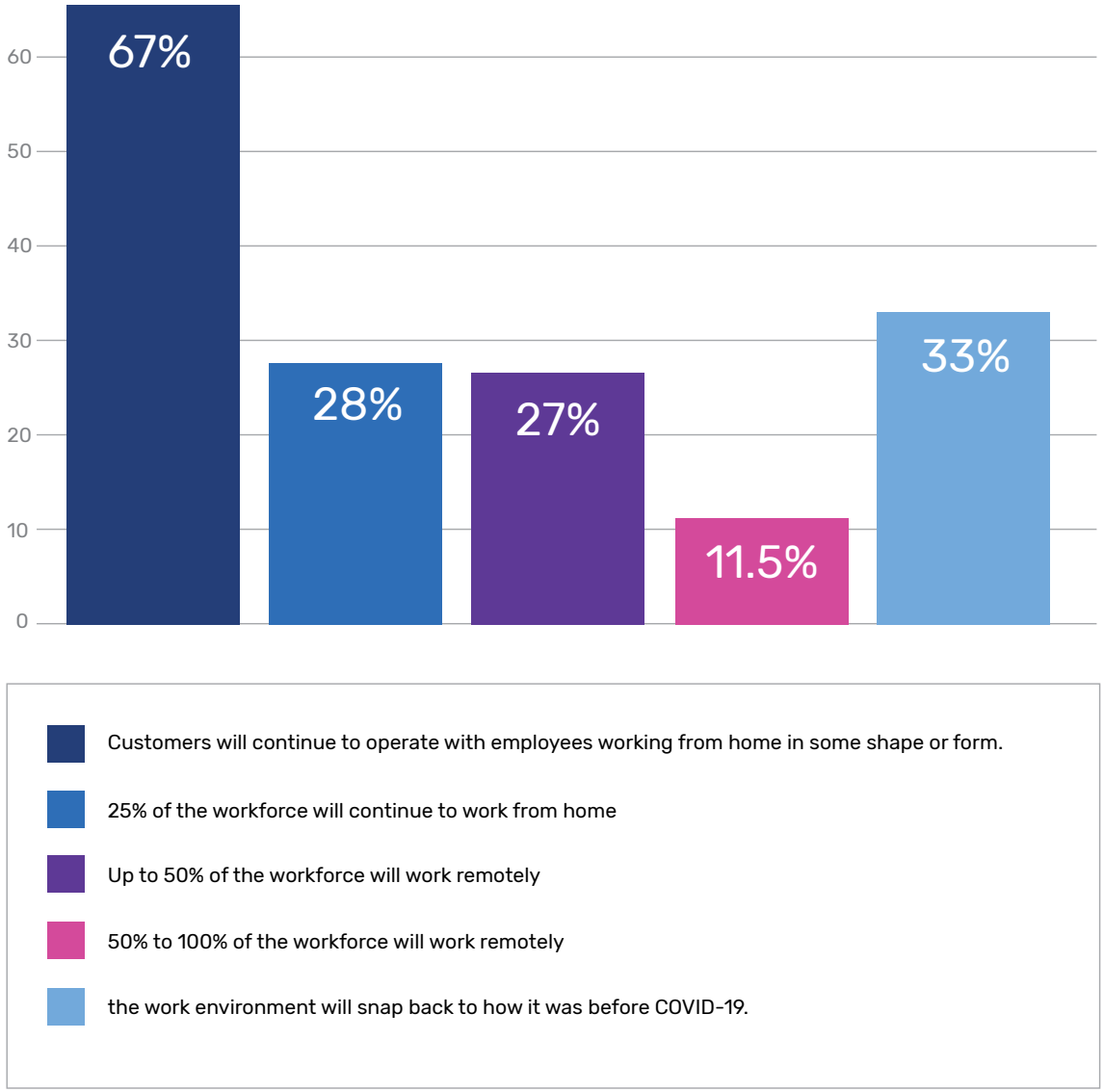
How, if at all, has COVID-19 most changed the relationship you have with your customers?



Over half (56%) of respondents have seen an increase in demand from their customers for online platforms such as customer service portals. Interestingly 52% of respondents claimed that customers are more concerned about business continuity and resilience than before the pandemic, and 44% of respondents said that customers have increased their security expectations around the network from communications service providers.

This is probably one of the reasons why 47% of communications service providers have changed their capital investment plans to invest in security. Overall, 44% said that they now have a larger pool of customers/subscribers to deal with and just under one-fifth (18%) said that customers are now in more diverse locations.

Do you think the work environment will snap back to how it was before the COVID-19 pandemic or will we see an evolution in how your customers/subscribers work?

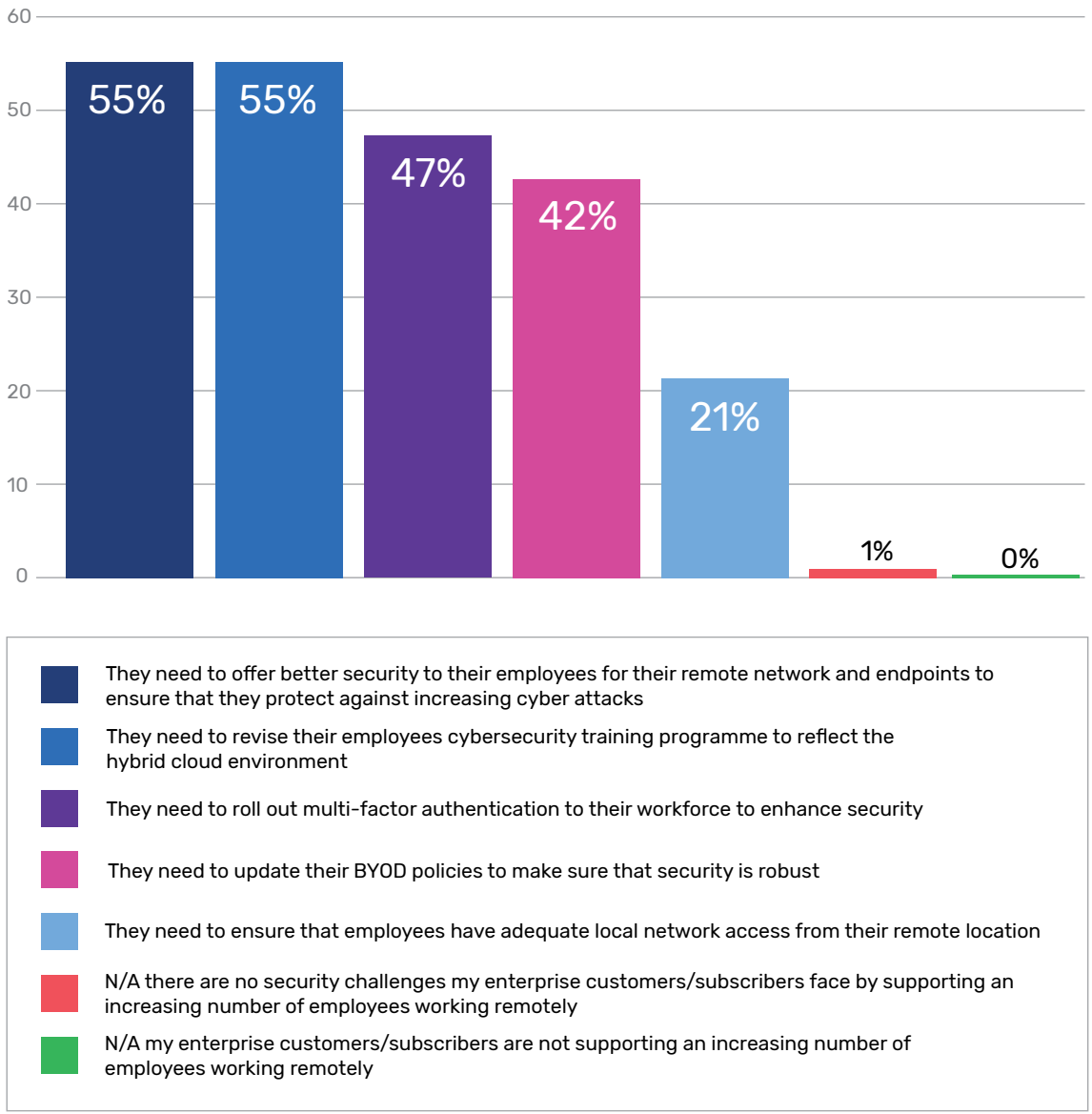


More than two-thirds (67%) of respondents believe their customers will continue to operate with employees working from home in some shape or form. 28% believe that 25% of the workforce will continue to work from home, 27% believe up to half the workforce working remotely and 11.5% say anywhere between 50% to 100% of the workforce could continue to work remotely post-pandemic.

Only one-third (33%) of respondents believe that the work environment will snap back to how it was before COVID-19.

Respondents serving the financial services market (40%) were most likely to believe the work environment will snap back to how it was. Interestingly, those respondents servicing the gaming industry thought that this sector was most likely to see a hybrid approach to work with three-quarters (75%) stating this.

What, if any, security challenges are your enterprise customers/subscribers facing if they are supporting an increasing number of employees working remotely?

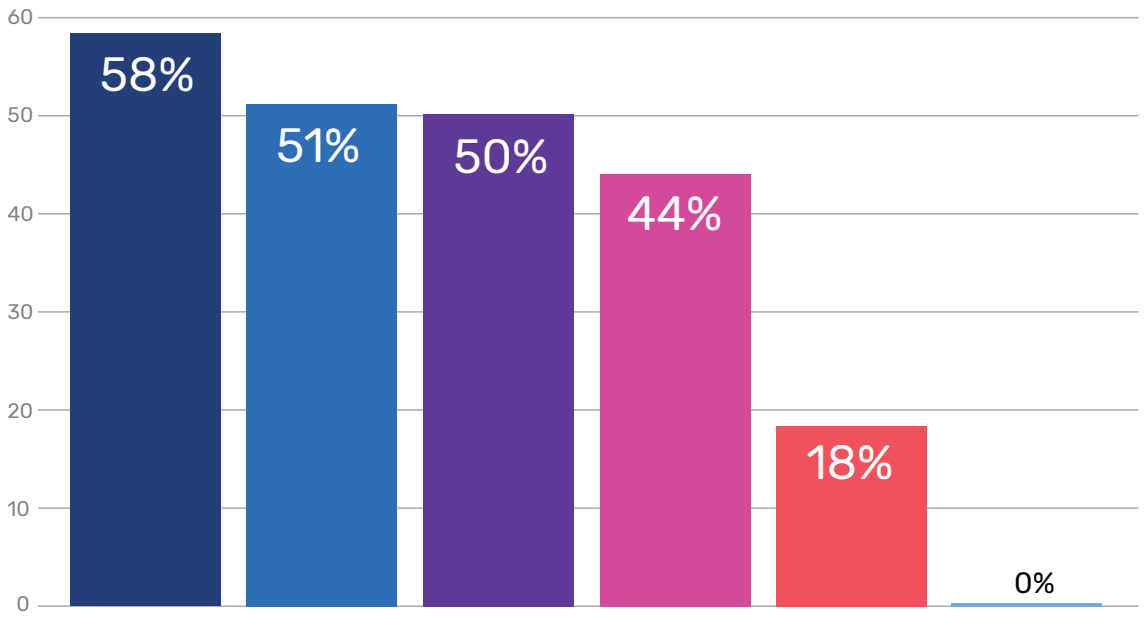


More than half of respondents say their customers have a requirement for better endpoint security (55%) to protect them against increasing cyber-attacks. Clearly, companies need to get the basics right in terms of having good endpoint security because organisations will only be as secure as the home networks they are on.

55% stated that their customers are looking to revise their employee cybersecurity training programme to reflect the hybrid working environment, and 47% stated that their customers would need to roll out multi-factor authentication to their workforce to enhance security. 42% say they need to update their BYOD policies to make sure their security is robust.

Both the education (62%) and healthcare (61%) sector-focused respondents say that their customers need to revise their employee cybersecurity training programmes. The financial services sector ranked highest in terms of their customers needing to ensure that BYOD policies were more robust.

What changes, if any, have you seen from your enterprise customers in their purchasing strategy for network services over the last year?

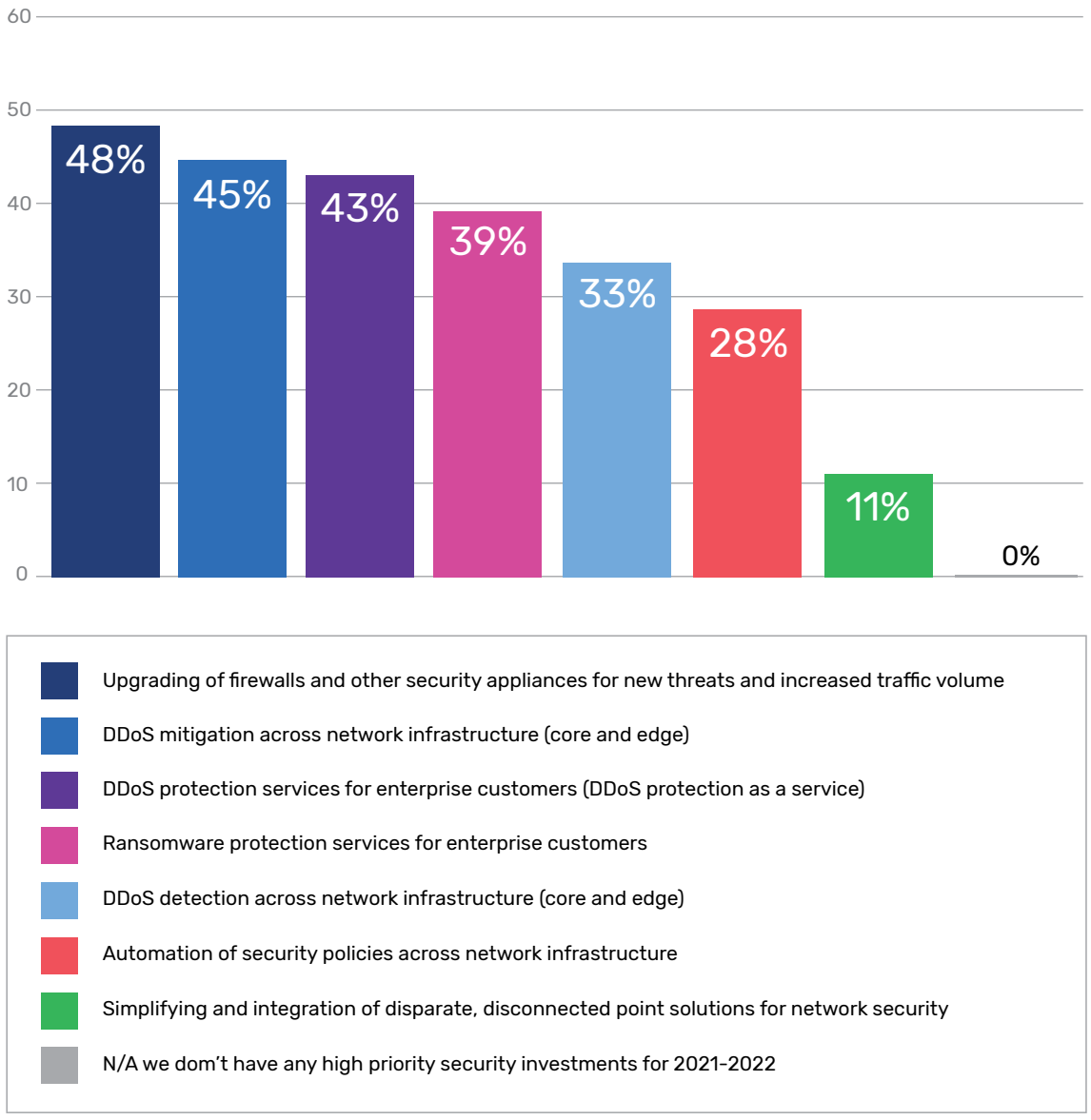


- They are splitting workloads and traffic between traditional telcos and non-telco cloud platform providers to reduce dependence on a single network vendor and minimise risk to service availability
- They are requiring end-to-end security SLAs across cloud and data centre for any chosen vendor
- They have expanded their telco vendor RFP list to include non-telcocloud platform providers (e.g., Google, AWS, Alibaba, Microsoft
- They are exploring private LTE or 5G options
- They are now willing to pay a premium for security services from their chosen vendor
- N/A there are no changes that I have seen from my enterprise customers in their purchasing strategy for network services over the last year

More than half (58%) of respondents stated they have seen their enterprise customers splitting workloads and traffic between traditional telcos and non-telco cloud platform providers to reduce their dependence on a single network vendor and minimise risk to service availability.

50.5% of respondents are seeing customers requiring end-to-end security SLAs across cloud and data centers for any chosen vendor. 50% also stated that customers have expanded their telco vendor RFP list to include non-telco cloud platform providers (for example Google, AWS, Alibaba and Microsoft).

What, if any, are your highest priority security investments for 2021-2022?



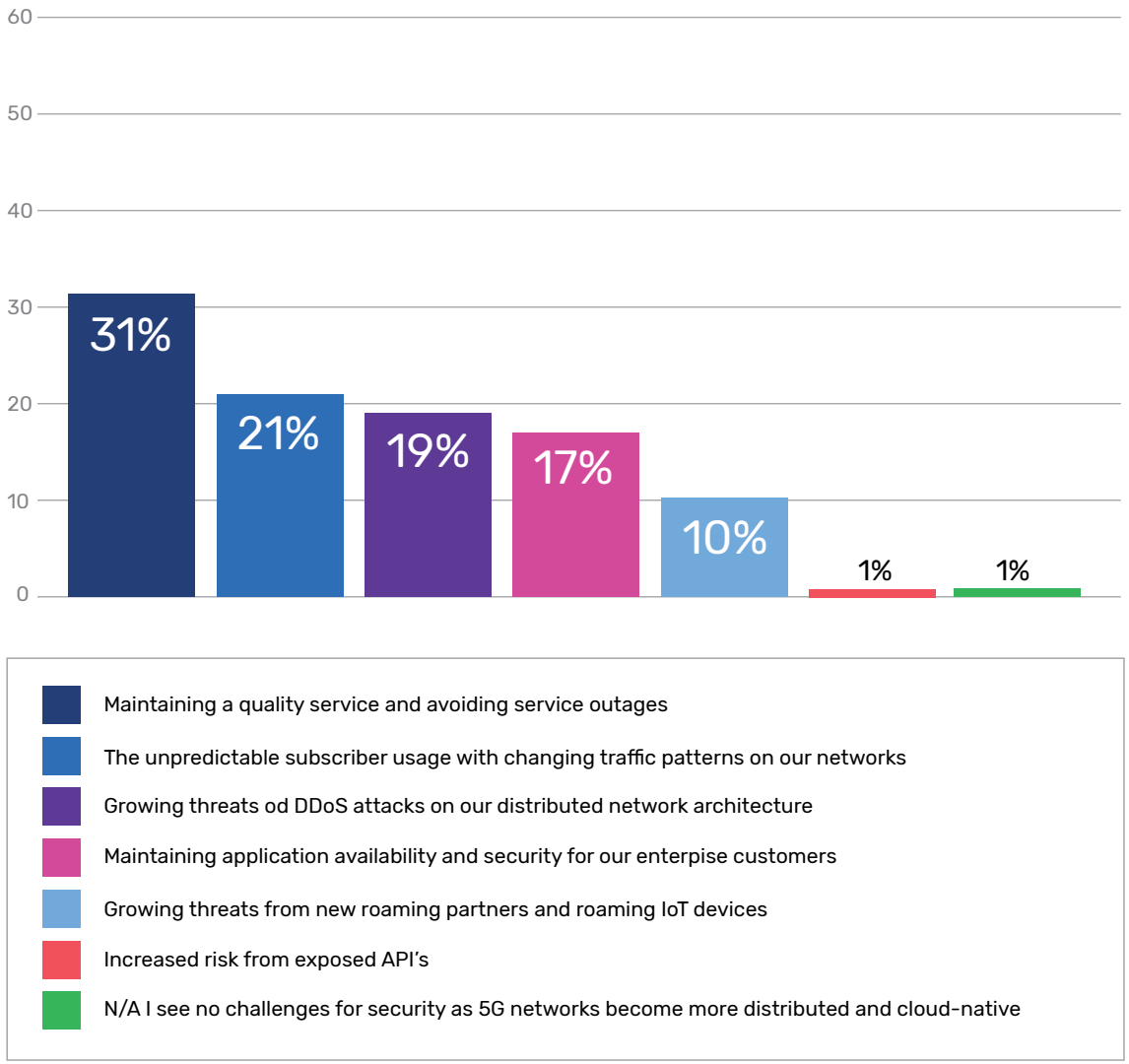
Just under half (48%) of providers stated that upgrading firewalls and other security appliances for new threats and increased traffic volume was their highest priority security investment in the next two years.

45% of respondents stated that DDoS mitigation across network infrastructure (core and edge) was a top priority. Respondents serving the education sector had this as a top priority (52%).

43% stated that DDoS protection service for enterprise customers (i.e., DDoS protection as a service) was a priority.

39% of communications service providers said ransomware protection services for enterprise customers was their highest priority.

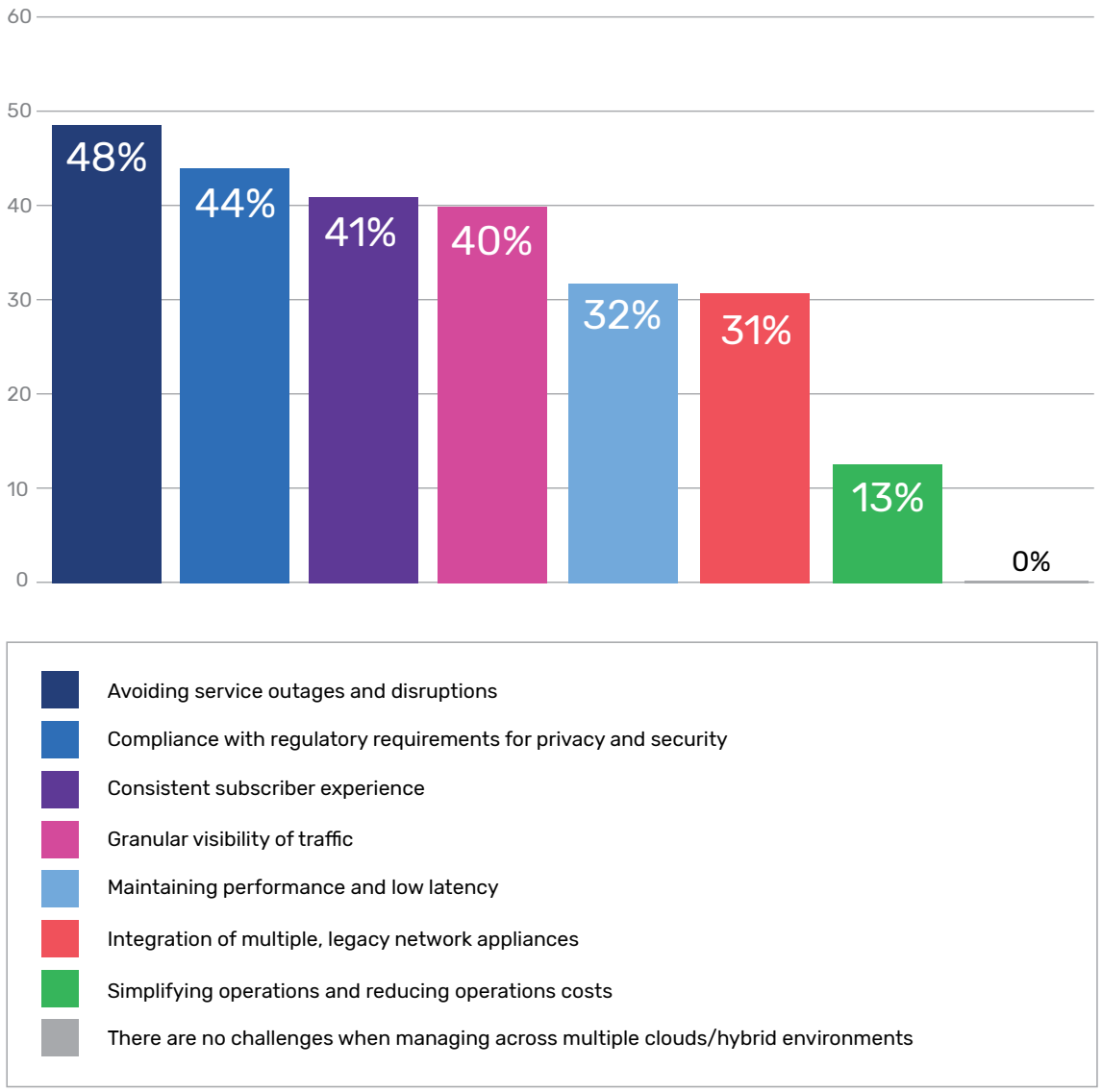
What, if anything, is the top security challenge you see as 5G networks become more distributed and cloud-native?



When it comes to 5G, just under one-third of respondents (31%) stated that maintaining a quality service and avoiding service outages were top security challenge. While 21% said a top challenge was the unpredictable subscriber usage with changing patterns on the network. 19% of respondents said growing threats of DDoS attacks on the distributed network architecture was a top challenge. 17% of communications service providers were concerned about maintaining applications and security for their customers as 5G networks become more distributed and cloud native.

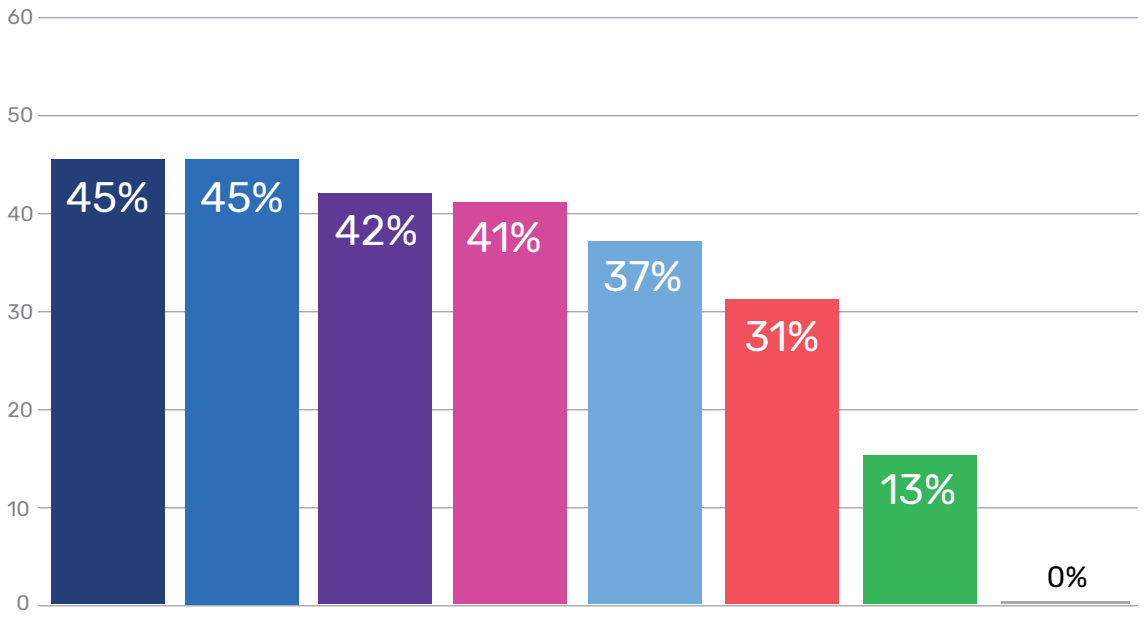
Clearly, for ecommerce and retail respondents ensuring uptime is critical and 35% said that maintaining a quality service and avoiding service outages were key challenges where 5G networks are concerned. Whereas 28% of gaming companies saw the unpredictable subscriber usage and the changing patterns on the network as their top security challenges.

What, if any, are the top-three main challenges when managing across multiple clouds/hybrid environments?



When it comes to the top-three challenges, communications service providers stated avoiding service outages and disruptions (47.5%) was the top challenge. Second was compliance with regulatory requirements for privacy and security (43.5%). Consistent subscriber experience (41%) when managing across multiple cloud and hybrid environments ranked as their third top challenge.

With ransomware, phishing and DDoS attacks growing exponentially, what, if any, additional capabilities and technologies will you need in 2021-2022 to protect your customer/subscriber networks from cyber-attacks, especially those that threaten network availability?



- Granular (Customer-level) DDoS Mitigation
- Increased security automation including automated policy support
- Application-layer visibility of customer traffic to detect malware
- Endpoint security
- Granular (customer-level) DDoS detection
- Common approach to security logging and monitoring across all network functions
- Advanced and automated detection mechanisms using machine learning
- N/A we have no plans to employ additional capabilities and technologies in 2021-2022 to protect our customer/subscriber networks from cyber attacks, especially those that threten network availability

In terms of additional capabilities to better protect customers and subscribers against growing threats, granular (customer level) DDoS mitigation was a top concern at 45%. This is probably why DDoS mitigation was stated as a top security investment requirement in response to question 9. Increased security automation including automated policy support was the second most popular choice for all communications service providers and was ticked by 45% of respondents. Application-layer visibility of customer traffic to detect malware (42%), and endpoint security (41%) were in fourth and fifth place.

COUNTRY COMPARISONS

At-a-glance Responses Across the Five Surveyed Countries

	UK	Germany	France	Middle East	India
Experienced increased demand for data and network bandwidth due to COVID-19	98%	100%	100%	99%	98%
Have had to scale up infrastructure in specific, high demand locations	60%	57%	47%	50%	59%
Reduced investment in own network and accelerated use of public cloud	48%	58%	58%	47%	39%
Have paused investment plans	59%	42%	50%	49%	45%
Believe customers will continue to have employees working from home long term	72%	74%	93%	66%	30%
Say customers are having to offer better network and endpoint security to protect against increasing attacks	61%	64%	54%	48%	48%
Say customers have expanded telco vendor RFP list to include non-telco cloud providers	32%	53%	34%	61%	71%
Are prioritising investment in upgrading firewalls and other security appliances for new threats and increased traffic	54%	56%	38%	43%	49%

COVID-19 has had a significant impact on all five countries that we surveyed. Germany and France tied at the top with 100% of respondents reporting an increase in demand as a result of COVID-19. The Middle East was in third place with 99%, and the UK and India were joint fourth with 98%.

In terms of how this increase in demand has affected business for communications service providers, the UK ranked highest in the need to scale up its infrastructure across the entire network (61%) and scaling up to meet specific high-demand (60%). Whereas Germany reported highest in investing in security technologies (49%), while France (54%) focused on redistributing network capacity to accommodate changes in demand. In India, the focus was on increasing headcount to meet this new demand (48%).

When asked whether the pandemic had accelerated a move to a more distributed network, 100% of French respondents claimed that COVID-19 had hastened this in some shape or form.

The pandemic has hit the UK hard, and this was reflected in respondents' answers around investment plans. The UK reported the highest on pausing investments (59%). This was followed by France (50%) and then the Middle East (49%). Interestingly, 70% of respondents from India are planning to increase investment in their own network.

Whereas both France and Germany (58% respectively) have reduced investment in their own network and accelerated use of public clouds.

In terms of how this has changed their relationship with customers, France ranked highest in seeing increased demand from customers for online platforms (61%). In the UK, customers are more concerned about business continuity and resilience (60%). 69% of respondents from India stated that customers are now more concerned about security, which was highest out of all five countries.

Interestingly, 70% of respondents from India believe that the workplace will snap back to how it was before the pandemic, in contrast with only 7% of French respondents. France reported the highest (93%) on continuing to operate with some form of home/ remote working post-pandemic, followed by Germany with 74%.

When it comes to security investments in the year ahead, both German (56%) and UK (54%) respondents reported the highest when asked about prioritising the automation of security policies across network infrastructure. More than half of Indian respondents see DDoS protection-as-a-service as a high priority (56%). This was also the highest priority for Middle East respondents (45%). French respondents reported their highest security priority is investing to protect against ransomware (48%).

COUNTRY REPORT: UK

Overview

COVID-19 has had a significant impact on service provider respondents in the UK.

98% of respondents said COVID-19 had created a more distributed environment on average by 44%. This has changed customer behaviour and:

- Increased demand for online platforms (51%)
- Amplified concerns around business continuity and resilience (60%)
- Increased expectations around security (36%)

The Workforce Won't Snap Back to How It Was

Only 28% say customers will return to pre-COVID-19 working practices, while 72% say remote working will continue in some form post pandemic.

Impact on Investment Plans

59% have paused their investment plans for the next 3 years

58% have accelerated investment plans in security

48% are investing less in their own network and moving to invest more in public cloud

Highest Priority Security Investments in 2021

Upgrade firewalls and security appliances (54%)

DDoS mitigation across network infrastructure (47%)

DDoS protection services for enterprise customers (40%)

250 UK respondents

98% say
COVID-19 increased
subscriber demand by an average of **53%**

This resulted in service providers having to scale up:

Network infrastructure	61%
In high demand locations	60%
Redistribute network capacity	48%
Investing more in security technologies	44%

Variations Compared With Other Countries

Out of the five countries, survey respondents in UK ranked highest in scaling up their infrastructure across the entire network (61%) and scaling up to meet specific high-demand locations (60%). Whereas Germany (52%) and France (54%) ranked above the UK (48%) for redistributing network capacity to accommodate changes in traffic demand.

Clearly, the pandemic has had a big impact on confidence as UK respondents ranked highest on pausing investments (59%), whereas all the other countries ranked higher than the UK for planning to increase investment in their own network. After India, the UK ranked highest in increasing investment in security (58%).

The UK ranked higher than the other four countries for increased customer concern around business continuity and resilience (60%) and enterprise customers demanding end-to-end security SLAs across cloud and data centres for any chosen vendor (57%).

COUNTRY REPORT: GERMANY

Overview

COVID-19 has had a significant impact on service provider respondents in Germany.

99% of respondents said COVID-19 had created a more distributed environment on average by 48%. This has changed customer behaviour and:

- Increased demand for online platforms (56%)
- Recorded an increased pool of subscribers (49%)
- Amplified concerns around business continuity and resilience (48%)

The Workforce Won't Snap Back to How It Was

Only 26% say customers will return to pre-COVID-19 working practices, while 74% say remote working will continue in some form post pandemic.

Impact on Investment Plans

58% are investing less in their own network and moving to invest more in public cloud

51% have accelerated investment plans in security

49% plan to increase investment in networks

Highest Priority Security Investments in 2021

Upgrade firewalls and security appliances (56%)

DDoS mitigation across network infrastructure (48%)

Ransomware protection services for enterprise customers (44%)

251 German respondents

100% say
COVID-19 increased
subscriber demand by an average of **56%**

This resulted in service providers having to scale up:

Network infrastructure	» 55%
In high demand locations	» 57%
Redistribute network capacity	» 52%
Investing more in security technologies	» 49%

Variations Compared With Other Countries

Out of the five countries, survey respondents in Germany ranked highest in their plans to reduce investment in their own network and accelerate use of public cloud providers (58%) and 49% of respondents also plan to accelerate their network transition to a more distributed network. Additionally, the demand for online platforms (56%) and the larger pool of customers that companies have to deal with (49%) shows that the German respondents face large-scale disruption due to COVID-19.

The increased demand for data and network bandwidth in Germany (69% stated that it increased over 50% and up to 100%) shows that companies are adapting to the new normal and the associated demands around remote working. Any changes in capital investment flows (only 42% say they have paused their investments) are mainly around long-term investments that include reorientation. German companies have thus realised that they need to invest in cloud providers (58%) or in their own networks (49%) in order to remain competitive in the future. The topic of investment in security was also high on the agenda (51%). In particular, German respondents ranked highest in saying that their customers are having to offer better network and endpoint security to protect against increasing attacks.

COUNTRY REPORT: FRANCE

Overview

COVID-19 has had a significant impact on service provider respondents in France.

100% of respondents said COVID-19 had created a more distributed environment on average by 47%. This has changed customer behaviour and:

- Increased demand for online platforms (61%)
- Amplified concerns around business continuity and resilience (45%)
- Increased expectations around security (25%)
- Increased the overall pool of subscribers (42%)

The Workforce Won't Snap Back to How It Was

Only 7% say customers will return to pre-COVID-19 working practices, while 93% say remote working will continue in some form post pandemic.

Impact on Investment Plans

58% are investing less in their own network and moving to invest more in public cloud

50% have paused their investment plans for the next 3 years

39% have accelerated investment plans in security

Highest Priority Security Investments in 2021

Ransomware protection services (48%)

Upgrading firewalls and security appliances (38%)

Automation and security policies across network infrastructure (36%)

250 French respondents

100% say
COVID-19 increased
subscriber demand by an average of **59%**

This resulted in service providers having to scale up:

Redistribute network capacity	54%
Network infrastructure	51%
Investing more in security technologies	48%
In high demand locations	47%

Variations Compared With Other Countries

Out of the five countries, survey respondents in France recorded the highest responses around remote working continuing in some form after the pandemic (93%), compared to Germany (74%), UK (72%) and Middle East (66%). It is the complete opposite for India where 70% of the respondents think the work environment will snap back to how it was before COVID-19. Likewise, French respondent customers were likely to have expanded their RFP list to include non-telco cloud providers (34%) versus India who are most likely (71%). It is interesting to see that European respondents have listed the same top-three security challenges their enterprise customers/subscribers are facing to support an increasing number of employees working remotely: first, the need to offer better security to their employees for their remote network and endpoints to protect against increasing cyber-attacks (France - 54% / Germany - 64% / UK – 61%) ; second, the need to revise employee cybersecurity training programmes to reflect the hybrid working environment (France - 52% / Germany - 55% / UK – 53%) and third, the need to roll out multi-factor authentication to their workforce to enhance security (France - 43% / Germany - 45% / UK – 51%).

COUNTRY REPORT: MIDDLE EAST

Overview

COVID-19 has had a significant impact on service provider respondents in the Middle East.

99% of respondents said COVID-19 had created a more distributed environment on average by 46%. This has changed customer behaviour and:

- Increased demand for online platforms (52%)
- Amplified concerns around business continuity and resilience (52%)
- Increased expectations around security (43%)

The Workforce Won't Snap Back to How It Was

34% say customers will return to pre-COVID-19 working practices, while 66% say remote working will continue in some form post pandemic.

Impact on Investment Plans

51% have accelerated investment plans in security

49% have paused their investment plans for the next 3 years

47% are investing less in their own network and moving to invest more in public cloud

Highest Priority Security Investments in 2021

DDoS protection services for enterprise customers (45%)

DDoS mitigation across network infrastructure (44%)

Upgrade firewalls and security appliances (43%)

250 Middle East respondents

99% say
COVID-19 increased
subscriber demand by an average of **52%**

This resulted in service providers having to scale up:

Network infrastructure	50%
In high demand locations	50%
Investing more in security technologies	48%
Redistribute network capacity	38%

Variations Compared With Other Countries

Out of the five countries, survey respondents in the Middle East lagged behind and ranked lowest in scaling up their infrastructure across the entire network (50%) in response to increased demand for data and network bandwidth from customers. Middle East ranked highest after India in terms of optimism about the work environment snapping back to how it was before COVID-19 (34%). In India, this figure was more than double (70%). Compared to the other countries, 'DDoS protection services for enterprise customers' and 'DDoS detection across network infrastructure' ranked very high when it comes to priority security investments for 2021-2022 for service providers in Middle East (45% and 42% respectively), which demonstrates that DDoS attacks are on the rise in the region and is emerging as a key threat vector. As 5G networks become more distributed and cloud-native, Middle East respondents are most confident in maintaining a quality service and avoiding service outages as compared to all the other countries, with only 21% seeing it as being a challenge. This goes to show that service providers in the Middle East believe they have good 5G security solutions and policies in place.

COUNTRY REPORT: INDIA

Overview

The pandemic has had a significant impact on service provider respondents in India. COVID-19 accelerated transition to a more distributed network in India, on an average by 47%. This has changed customer behaviour and:

- Increased demand for online platforms (60%)
- Amplified concerns around business continuity and resilience (54%)
- Increased expectations around security (69%)

The Workforce Won't Snap Back to How It Was

70% of customers will return to pre-COVID-19 working practices post pandemic and only 30% say that remote working will continue in some form post pandemic.

Impact on Investment Plans

62% have accelerated investment plans in security

39% are investing less in their own network and moving to invest more in public cloud

70% plan to increase investment in networks

45% have paused their investment plans for the next 3 years

Highest Priority Security Investments in 2021

Upgrade firewalls and security appliances (49%)

DDoS mitigation across network infrastructure (50%)

DDoS protection services for enterprise customers (56%)

250 India respondents

COVID-19 increased subscriber demand by an average of **54%**

This resulted in service providers having to scale up:

Network infrastructure	» 59%
In high demand locations	» 59%
Redistribute network capacity	» 38%
Investing more in security technologies	» 48%

India ranked highest in increasing their investments in security (62%), and networks (70%).

Variations Compared With Other Countries

Out of the five countries, India ranked the highest for experiencing an increased expectation from customers 'around security' from network service providers (69%), increased demand for online platforms such as customer service portals (60%) and increased customer concern around business continuity and resilience (54%). This is probably why the survey respondents in India ranked highest for witnessing an increase in their investments in security (62%), and networks (70%) and shifting investment to residential geographic locations (26%).

In just a year's time, the world has changed drastically as the COVID-19 pandemic has had and is continuing to have a deep impact on India as the respondents ranked lowest on accelerating the use of public cloud providers (39%), whereas all the other countries ranked higher than India. After the UK, India ranked highest in the need to roll out multi-factor authentication to their workforce to enhance security (50%). Survey respondents in India ranked much higher that other four countries, in revising employee cybersecurity training programme to reflect the hybrid working environment (64%).

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10networks.com and follow us @A10Networks.

Learn More

About A10 Networks

Contact Us

A10networks.com/contact

Part Number: A10-EB-14142-EN-01 MAR 2021