REPORT

April 2023

Global Communication Service Providers: Market Growth Fuels Security Investments

Global Communication Service Provider Insights 2023

Understanding the priorities, expectations, and perspectives of senior IT professionals in communication service providers across the globe.

Table of Contents

01.

Introduction

Global Communication Service Provider Insights 2023

This research was conducted to provide insight into the opportunities, challenges, and concerns facing communication service providers (CSPs) worldwide as they evolve and expand their services and infrastructure in an increasingly complex digital environment. It explores their plans for investment, the continuing impact of cloud migration, plans to address the digital divide and unserved/underserved communities and how they are approaching the IPv6 transition. The study also delves into how communication service providers are tackling the challenge of network security to support business growth.

Read this analysis to understand the priorities, expectations, and perspectives of senior IT professionals in communication service providers across the globe.

02.

Methodology

A10 Networks commissioned a survey, undertaken by an independent research organization, Opinion Matters, in January 2023. 2,750 senior IT professionals in communication service providers employing more than 250 people were surveyed.

Respondents came from a broad range of provider types and company sizes, including mobile operators, fixed-line telecom operators, cable operators, MVNO, MVNE with infrastructure, OTT service providers, data center/co-location service providers, and fixed wireless access providers.

This is the second A10 Networks survey of communication service providers, and expands on the previous study, which was conducted in 2021.

2,750 Respondents → in → 21 Countries

The markets surveyed were: United Kingdom, Southern Europe (France and Italy), United States, Germany, India, Middle East (UAE and Saudi Arabia), Benelux (Netherlands and Belgium), Central and Eastern Europe (Hungary, Czech Republic, Poland), Asia-Pacific (Australia, Hong Kong, Singapore), Nordics (Finland, Norway, Sweden), and Brazil and Mexico.

03. Executive Summary

A10 Networks' 2023 Global Communication Service Provider Insights research has revealed that:

Network security is becoming more sophisticated

Growth is expected and is driving investment plans

Providers are working to address the digital divide

Enterprise cloud migration is having a positive impact

Focusing on investment, preparing for growth, expanding services to meet underserved communities, and seizing opportunities are the four positive themes running through the results of the second global survey into the views of communication service providers.

As the world suffers considerable uncertainty stemming from economic, social, and geo-political disruption, digital connectivity has never been more important as a channel to address inequality, support communities, and drive global business recovery.

For the service providers responsible for delivering that connectivity, this environment is a double-edged sword. Commercial operating conditions are challenging, with supply chains suffering major ongoing disruption and finance becoming harder to secure. The cyber threat landscape continues to intensify, with cyber-attacks rising in frequency and volume as nation-state actors and conventional wage political and financial warfare across global digital ecosystems.

On the other hand, demand is robust. Although the pandemic-related traffic surge has abated, nearly all respondents expect to see healthy growth in traffic over the next two to three years.

As a result of this predicted growth, together with rising compliance obligations and the challenging cybersecurity landscape, almost all communication service providers are planning to invest in network security. There are also encouraging signs that the overall approach to security is maturing and becoming more sophisticated. In the 2021 survey, much of the planned investment focused on basic hygiene such as upgrading firewalls. Now, respondents are exploring a much more rounded and multi-layered

DDoS Cyber Attacks Intensify

15M

The number of DDoS weapons tracked by A10 Networks through 2022 is estimated at 15M

Microsoft Defense Report 2022 showed avg. of 1,955 attacks per day, up 40% YoY in 2022

defense-in-depth approach where DDoS detection and monitoring is a much higher priority, and is complemented with security policy automation, and ransomware and malware protection.

Alongside investing in network security, more than two-thirds of the organizations surveyed are planning to expand their network to reach unserved/underserved communities; a further third are building additional data centers to offer more capacity to other service providers. Connecting communities is central to reducing inequality and supporting digital opportunities, so it is heartening to see this positive direction. Combining this with a robust security strategy will result in more people and communities worldwide benefiting from safe, reliable digital services.

Among existing customers, the ongoing enterprise cloud transition has the potential to exert both positive and negative impacts on communication service providers, so it is interesting to find that one in four say they have gained revenue as customers have distributed workloads and data center functions among private, on-premises and public clouds.

On the topic of the IPv6 transition, the story is not as progressive. Globally, IPv6 adoptions has not progressed as quickly as hoped, and most traffic and web destinations are still IPv4 only. As a result, survey respondents generally favor a more cautious approach that leverages existing investment and carefully manages existing IPv4 addresses, or runs the two in parallel, rather than accelerating full transition plans to IPv6. Almost half of the respondents said they planned to acquire more IPv4 addresses through an existing provider or via the public market, a strategy that will become increasingly costly in the future.

Beyond this, communication service providers expect to encounter a range of business challenges as their networks evolve to new technologies and architecture. Among those identified are increased risk from exposed APIs as a result of app modernization, open source and AI, as well as supply chain challenges and threats arising from connected partner ecosystems and IoT. However, they also see opportunities resulting from increases in demand and further globalization; these include developing new services and expanding into new geographies to capitalize on market growth.

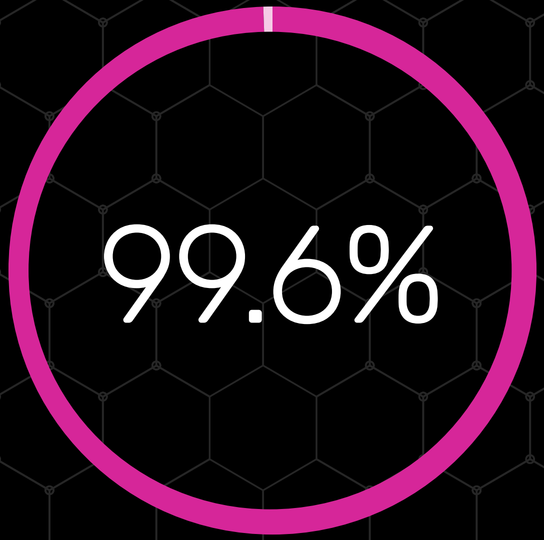
The second global communication service provider report includes analysis highlighting variations between territories as well as country and region snapshot summaries at the end of the report.

04.

Top Findings

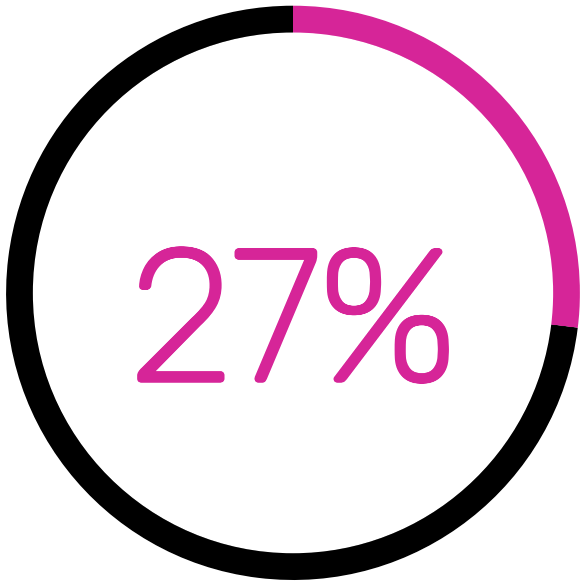
Robust Expectations of Market Growth Are Fueling Investment in Network Security

Almost all the communication service providers surveyed believe that robust growth in traffic volumes will continue in the coming two to three years — globally by a minimum of 25 percent. Almost half (48%) expect traffic will rise by between 50 percent and 75 percent, while one in five expect to see growth of more than 75 percent. The average global growth in traffic volumes expected is 58 percent worldwide. These predictions align with the sustained traffic growth generally seen in recent years and, although the pandemic generated a one-off burst, we are now seeing more sustained patterns emerging, showing growth at a considerable rate.



Of communication service providers surveyed believe that robust growth in traffic volumes will continue in the coming two to three years.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

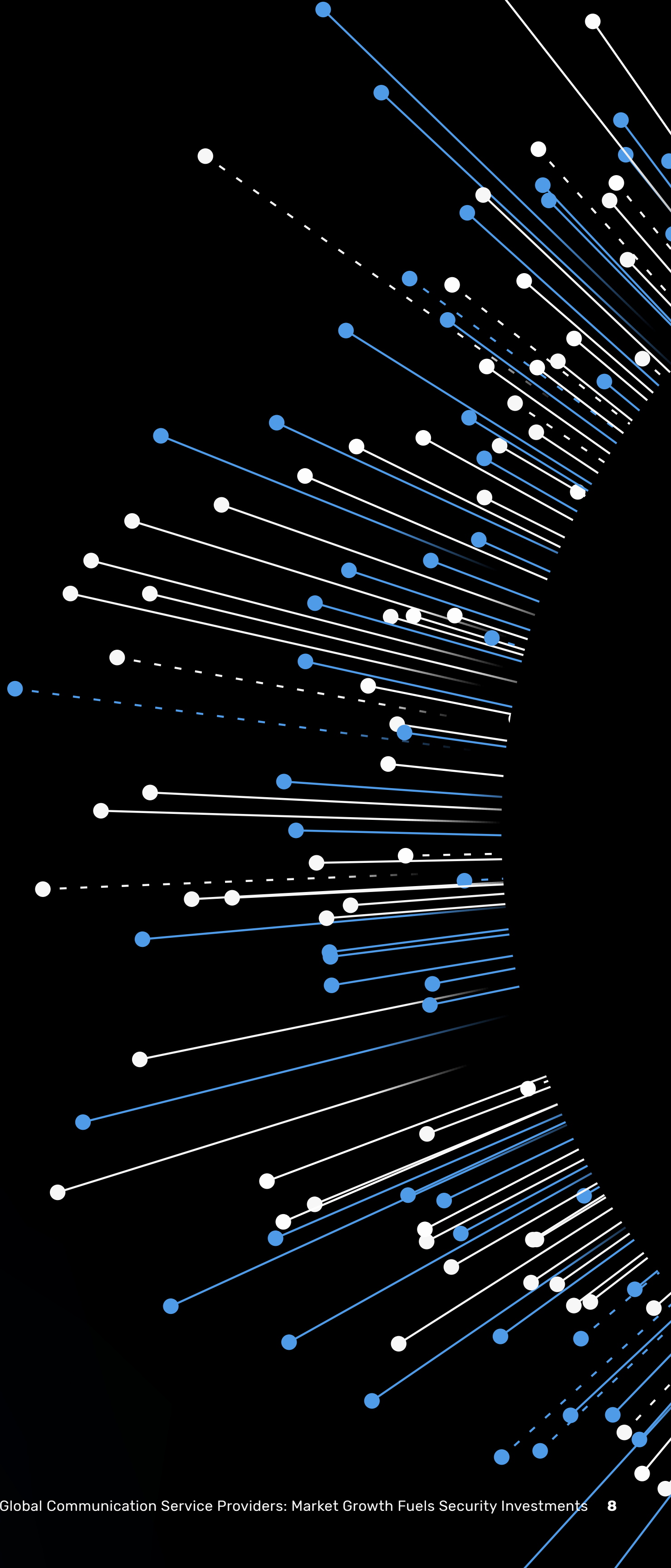


of respondents said that efficiency for climate issues was driving them to invest more in network security in the coming years.

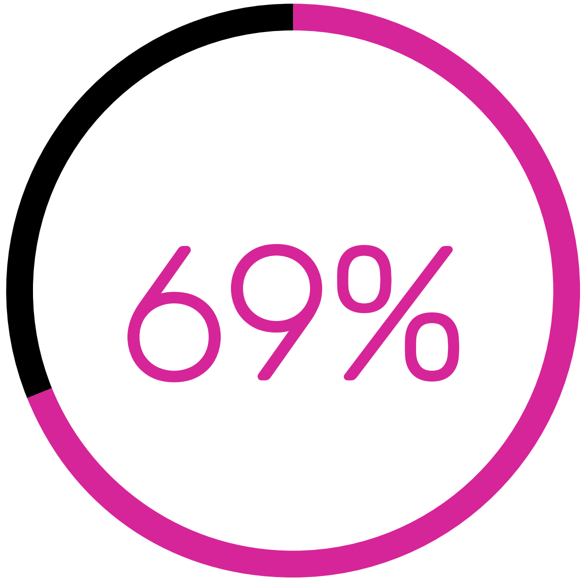
These positive growth levels create both the urgency and the confidence to undertake investment projects, a welcome change from the pandemic period, where investment was paused for half of organizations surveyed.

Now, respondents report that growth is the main driver for investment in network security. It is not the only factor, however. Government and regulatory reporting, together with security compliance pressure are also playing a part, alongside technology shifts and competitive pressure.

Interestingly, environmental issues are coming into play, as organizations recognize their responsibility to improve efficiency and reduce power consumption. More than one quarter (27%) of respondents said that efficiency for climate issues was driving them to invest more in network security in the coming years.



Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10



of respondents say they are expanding their networks to unserved/underserved communities.

Network Security Strategy is Becoming More Sophisticated and Diverse

When respondents were asked to identify their top priorities for network security investment, a broad range of activities were in the pipeline. The most commonly selected activity was upgrading firewalls and other security appliances for new threats and increased traffic, but compared to the 2021 research, this was less of a dominant focus.

Now, DDoS detection and monitoring is almost as high a priority, closely followed by automation of security policies, and ransomware and malware protection services. Respondents were also aiming to simplify and integrate disparate point security solutions and invest in threat intelligence capabilities.

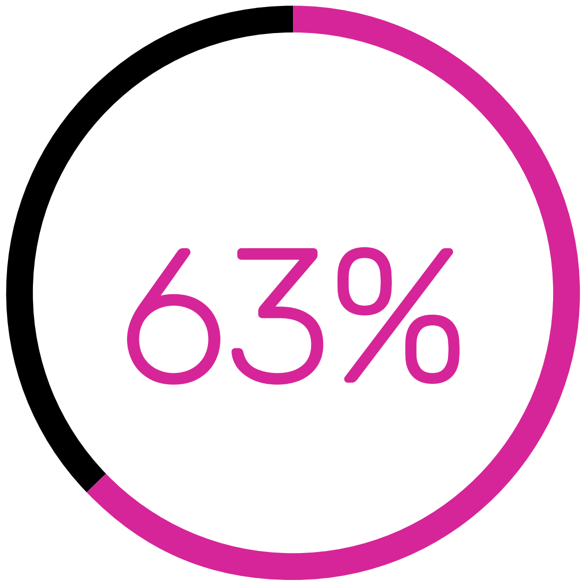
This points to the realization that today's network security strategy must be wide-ranging and multi-faceted, with a well-rounded approach that can manage the full spectrum of emerging threats to maintain reliable, high-quality services for customers

Providers are Working to Close the Digital Divide

Overall, 69 percent of respondents say they are expanding their networks to unserved/underserved communities. Half are anticipating a subscriber uplift of more than 10 percent of their current subscriber base and 19 percent expect an uplift of more than 50 percent of their current subscriber base. A further 31 percent — typically composed of respondents from larger businesses — said that their focus was on building out additional data centers and expanding to provide additional capacity to other service providers.

As awareness of the digital divide has grown and the socio-economic impacts of low or no internet connectivity are better understood, governments are incentivizing providers to deliver services in areas previously judged commercially unviable. These incentives are typically aimed at smaller providers that see opportunities in building a community-focused customer base.

Larger companies are prioritizing building data centers due to their high profitability, putting them in a strong position to provide infrastructure to those smaller service providers. So, while they are not directly building out to these communities, they are providing infrastructure and capacity to those smaller CSPs that are. In combination, this should see a reduction in the digital divide and the accompanying economic and social benefits that governments and communities are seeking, which will be fundamental to economic recovery.



of respondents report a positive outcome related to the cloud transition.

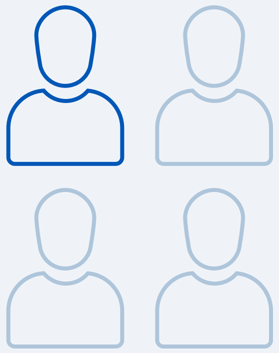
Enterprise Cloud Migration has a Silver Lining

Enterprise migration to the cloud has been a strong trend over the past decade, accelerating during the pandemic as organizations sought to support home and hybrid workers. Many enterprises are now focused on finding the right mix of cloud services to support their future plans.

Overall, 63 percent report a positive outcome related to the cloud transition. One in four say they have gained revenue as customers distribute workloads and data center functions among private, on-premises and public clouds. A further 20 percent say they have evolved to offer public cloud and managed data center services, and 19 percent say their differentiated services have increased relevance to customers.

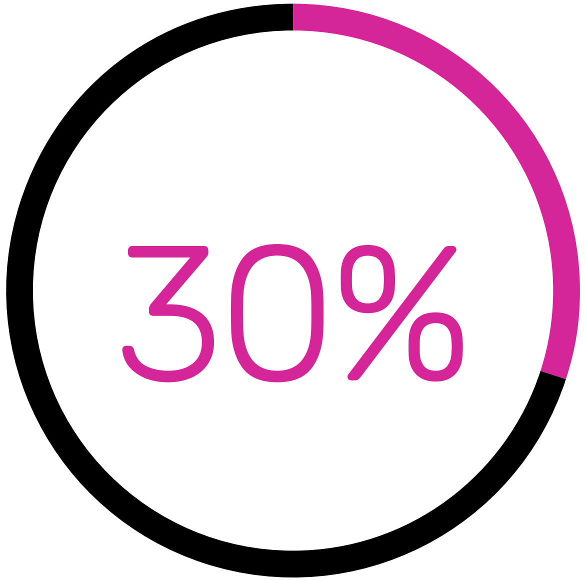
Of the remainder, one in five say their customers prefer on-premises solutions and are not moving to public or private cloud. Only 16 percent say they have lost revenue as enterprise customers move to public cloud providers.

The cloud transition is also evident when it comes to key purchase criteria for network equipment, a cloud-native form factor is a must-have. Integration with existing operations support systems is also a key feature, indicating that organizations are aiming to leverage earlier investment as they evolve networks for the future.



One in four say they have gained revenue as customers distribute workloads and data center functions among private, on-premises and public clouds.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10



of respondents expect to transition to IPv6 in the next two to three years.

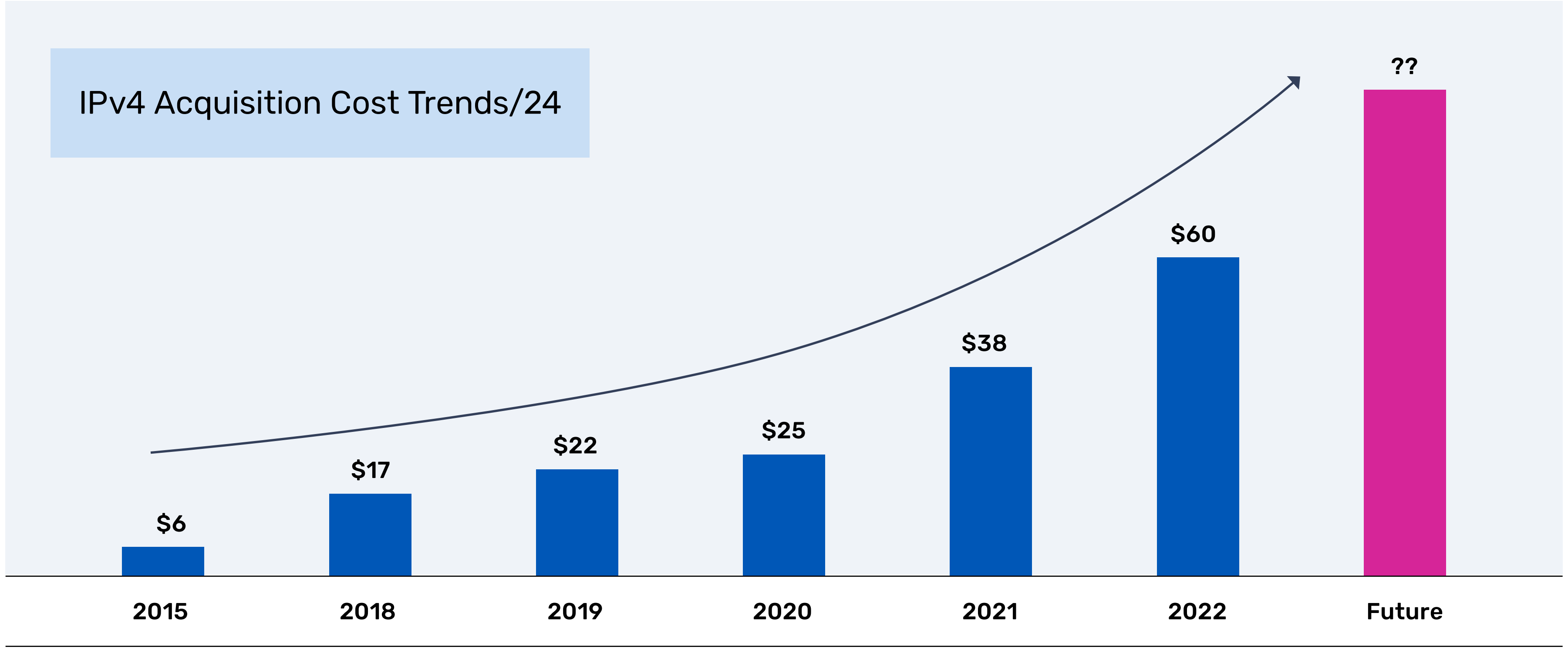
The IPv6 Transition Remains an Ongoing Challenge

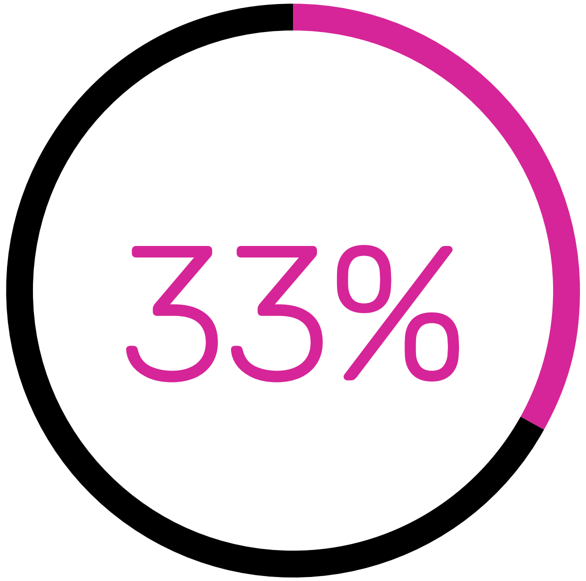
Worldwide, demand from service providers as they add more previously unconnected subscribers and IPv4 acquisition by global cloud providers has made IPv4 addresses into a very scarce resource. Providers need to plan for transition to IPv6, but the survey shows that only 30 percent expect to achieve this in the next two to three years.

More than one-third are adopting a strategy of carefully managing their IPv4 address pools and gradually transitioning to IPv6, while 34 percent aim to run the two in parallel.

In terms of strategies to manage IPv4 address shortages for those not yet making a full transition, options range from using CGNAT to manage existing allocations, acquiring more IPv4 addresses from another service provider and acquiring more IPv4 blocks on the public market.

This last option is growing increasingly costly, as scarcity continues to drive up prices towards the $60 mark and beyond.





of respondents say widespread supply chain struggles created shortages affecting their ability to meet their growth projections.

Despite Business Challenges, Opportunity Abounds for New Services as Demand Stays Strong

The survey participants noted a range of challenges arising from both the prevailing cybersecurity environment and external macroeconomic factors as their networks evolve to new technologies and architectures. Of greatest concern for most organizations is the increased risk generated by exposed APIs as a result of application modernization, open source, and AI, but this is not the only concern.

The supply chain struggles that have been widespread in the past three years are also having an impact, with more than a third saying these have created shortages affecting their ability to meet their growth projections.

Rounding off the top-three business challenges is the task of maintaining quality service and avoiding service outages.

When asked where they see opportunities, many respondents sought to address the issue of delivering high-quality, reliable service, and planning to build or improve a DDoS cloud scrubbing service. Many also plan to expand their hosting offerings or launch new services.

Continued market globalization is also viewed as an area of potential, with 27 percent expecting this will allow them to enter new markets. All this is backed up by the expectation of continued demand and growth for internet and network bandwidth.

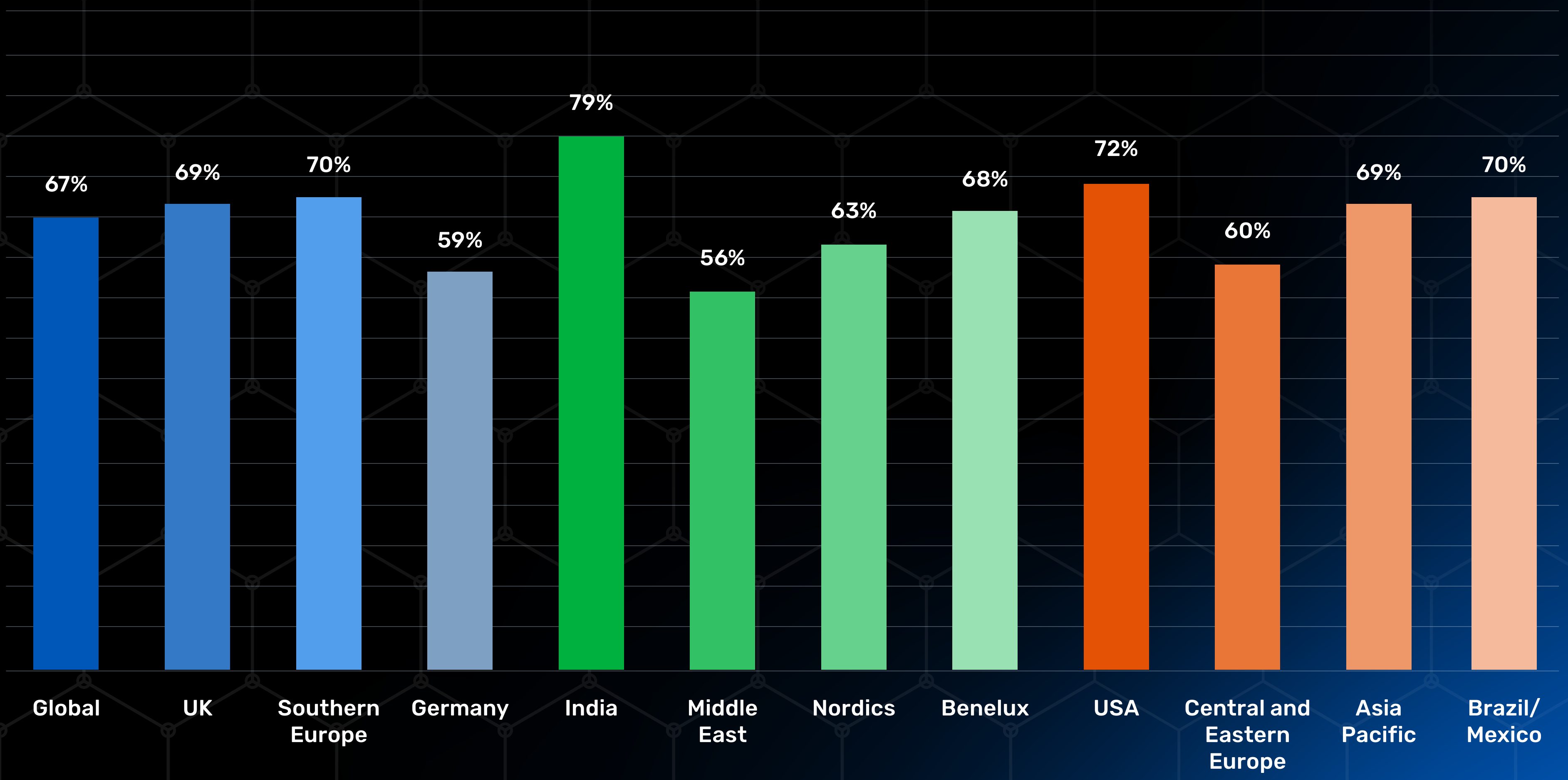
Overall, the research reveals a positive outlook for the global communication service provider community. Organizations are aiming to grow and improve services, expand into new markets, while maintaining robust and reliable services underpinned by sound network security investment.

Read on for detailed survey responses, country comparisons and country-specific analysis.

Full Survey Results

1. Over the next 2-3 years, how much do you expect network traffic volume from your customers/subscribers to increase, if at all?

Percentage of respondents predicting traffic increases of 50% or more



Two-thirds of respondents expect to see traffic increase of 50 percent or more, with almost one in five (18%) believing it will soar by 75 percent or more. Overall, 99.6 percent of respondents expect to see traffic rise in the next two to three years.

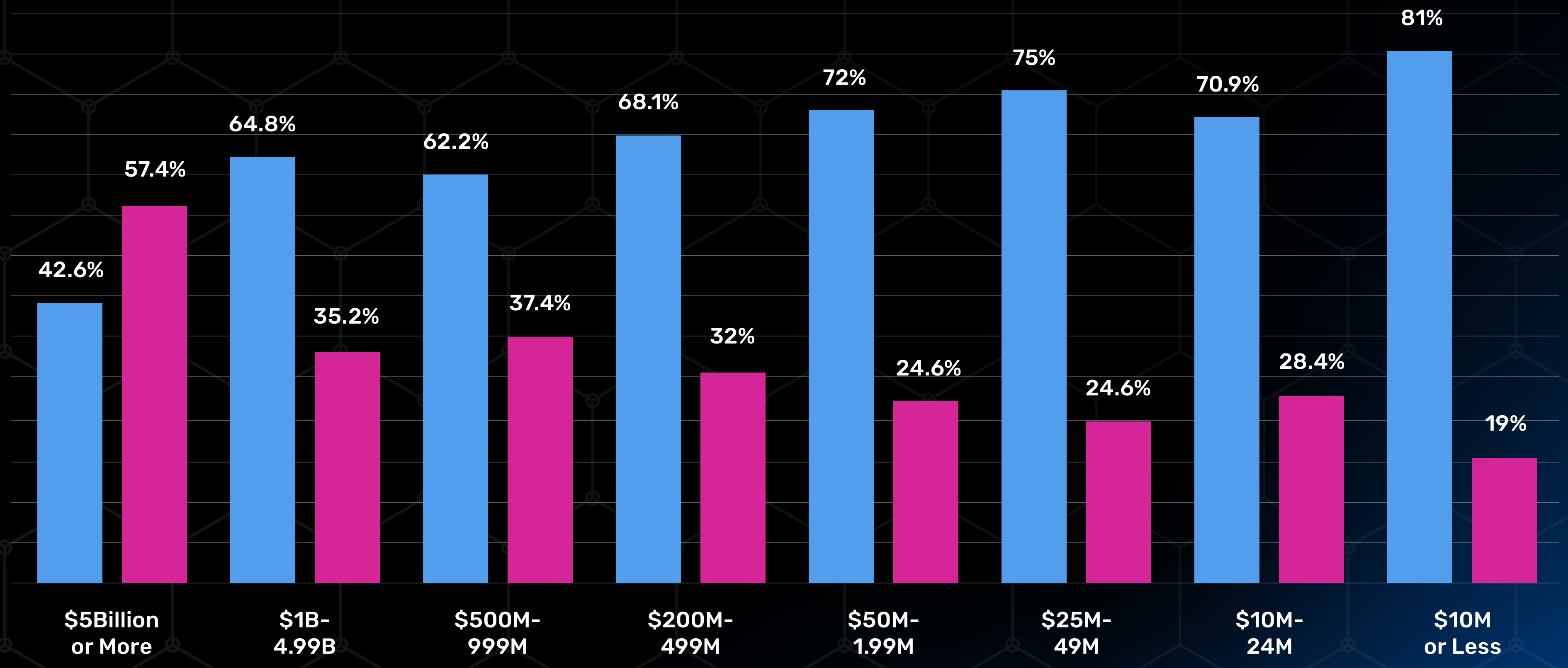
Respondents from India report the highest expected traffic increases on average at 64 percent, which may reflect the country's increased focus on delivering its flagship "Digital India" program, with the aim of delivering digital infrastructure as a core utility to every citizen. India is followed by the U.S. (61%) and UK (60%). Germany and Nordic countries have slightly lower expectations, although they still expect robust growth of 55 percent on average.

Empirical research into traffic levels indicates that while the pandemic demand surge was "a one-off phenomenon," traffic growth remains robust, albeit slowing slightly in recent years.[1] This research correlates with this general sentiment that volumes will continue to trend upward.

[1] "Global Internet Geography Research Service 2022", Telegeography, accessed at: Download the Global Internet Geography Executive Summary (telegeography.com)

Full Survey Results

2. Over the next 2-3 years, how will your build-out investments change to extend coverage to unserved/underserved communities, if at all?



🟦 We are expanding our network to unserved/underserved communities for an uplift of more than 10%/more than 50% of our current subscriber base

🟪 We are building out additional data centers and expanding to provide additional capacity to other service providers

How regional ISPs are bridging the digital divide through innovation

Regional ISPs play an important role in reducing the digital divide for customers in unserved/underserved locations.

Read this report from STL Partners, which highlights four key business model factors regional ISPs can consider to aid in building networks and services more quickly.

The good news is that all but ten respondents are planning to invest to extend coverage to unserved/underserved communities in one form or another. Half are planning to expand their networks for an uplift of more than 10 percent on their current subscriber base, while 19 percent are expanding for an uplift of more than 50 percent. The remaining 31 percent are planning to build additional data centers and expand to provide additional capacity for other service providers.

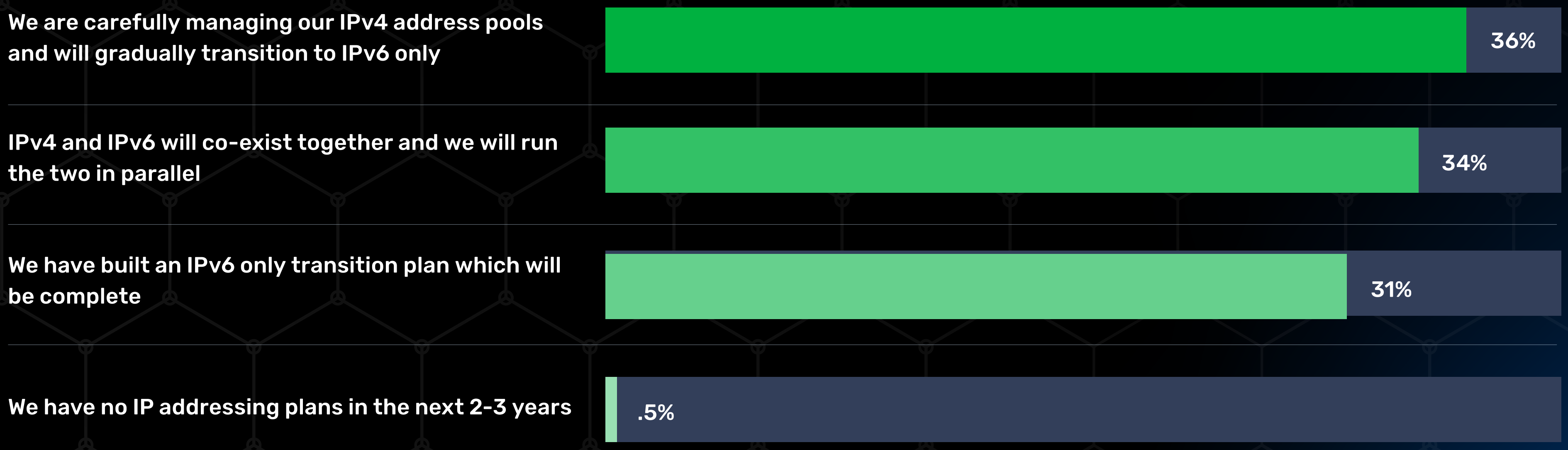
There are some significant variations in the approaches among the different geographies. In India, respondents are much more likely to be building out additional data centers and adding capacity, with 59 percent saying they are doing this compared with a global average of 31 percent. In contrast, 82 percent of respondents from the Middle East are expanding their networks for a subscriber uplift and only 16 percent are focusing on data center expansion. A mere 2.4 percent of respondents in this region are not planning any investment at all.

The impact of government incentives to extend coverage to more subscribers is likely behind the clear split in responses between smaller organizations, who are more likely to be expanding their networks, and large ones that are more likely to be building out data center capacity, as the graph demonstrates.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

Full Survey Results

3. Given the networking requirements for IPv4 and IPv6, what are your IP addressing plans in the next 2-3 years, if anything?



There is a lack of urgency around the IPv6 transition.

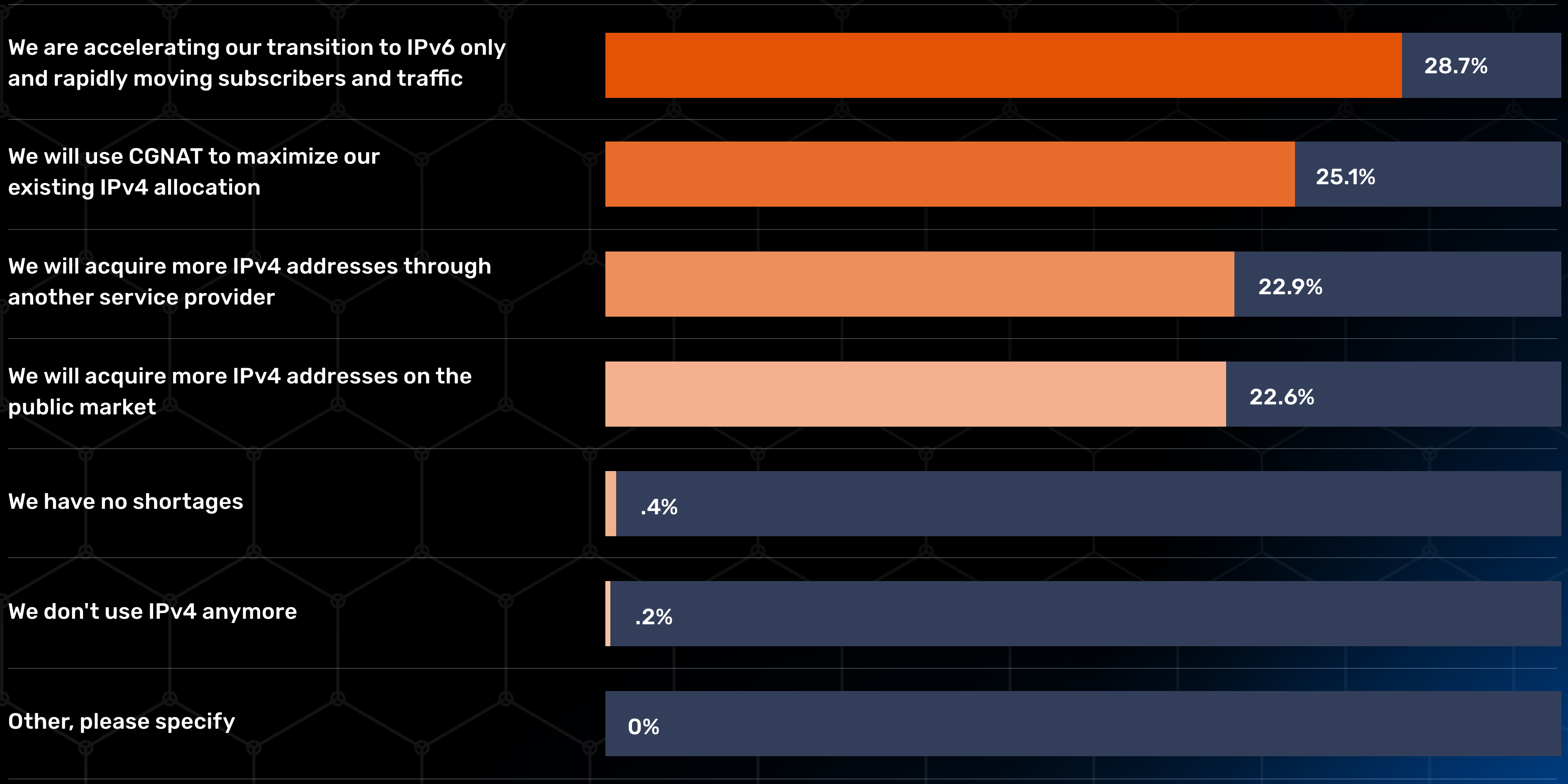
Many respondents (35%) said they were planning to carefully manage their existing IPv4 address pools and will gradually transition to IPv6, with this figure rising to 38 percent in Brazil and Mexico. However, almost the same proportion (34%) plan to have IPv4 and IPv6 co-existing in parallel. Although, again, Brazil and Mexico vary, with only 29 percent of respondents taking that approach. In the U.S., slightly more respondents than average (37%) plan to have IPv4 and IPv6 co-exist, while 33 percent say they are carefully managing IPv4 address pools.

31% of respondents say they will have completed the transition to IPv6 fully within the next two to three years.

Only 31 percent say they will have completed the transition to IPv6 fully within the next two to three years. This figure drops to 23 percent among respondents from India and rises to 35 percent in the Nordic region and 34 percent in the UK.

Full Survey Results

4. How are you addressing IPv4 shortages, if at all?



Addressing the IPv4 — IPv6 transition

Learn more about the challenges and strategies for managing IPv4 address exhaustion, and the opportunities for closing the digital divide, in this on-demand webinar with Dr. Sally Eaves **"Catch up or leap forward: Bridging the Digital Divide with A10"**

In terms of how communication service providers are currently addressing IPv4 shortages, the survey found that 29 percent are accelerating their transition to IPv6 only and rapidly moving subscribers and traffic. Respondents from the UK are more likely than other regions to be taking this approach (35%), while those in the Benelux and Asia-Pacific regions are less likely (both 24%). U.S. respondents aligned with the overall average, with 29 percent taking this approach.

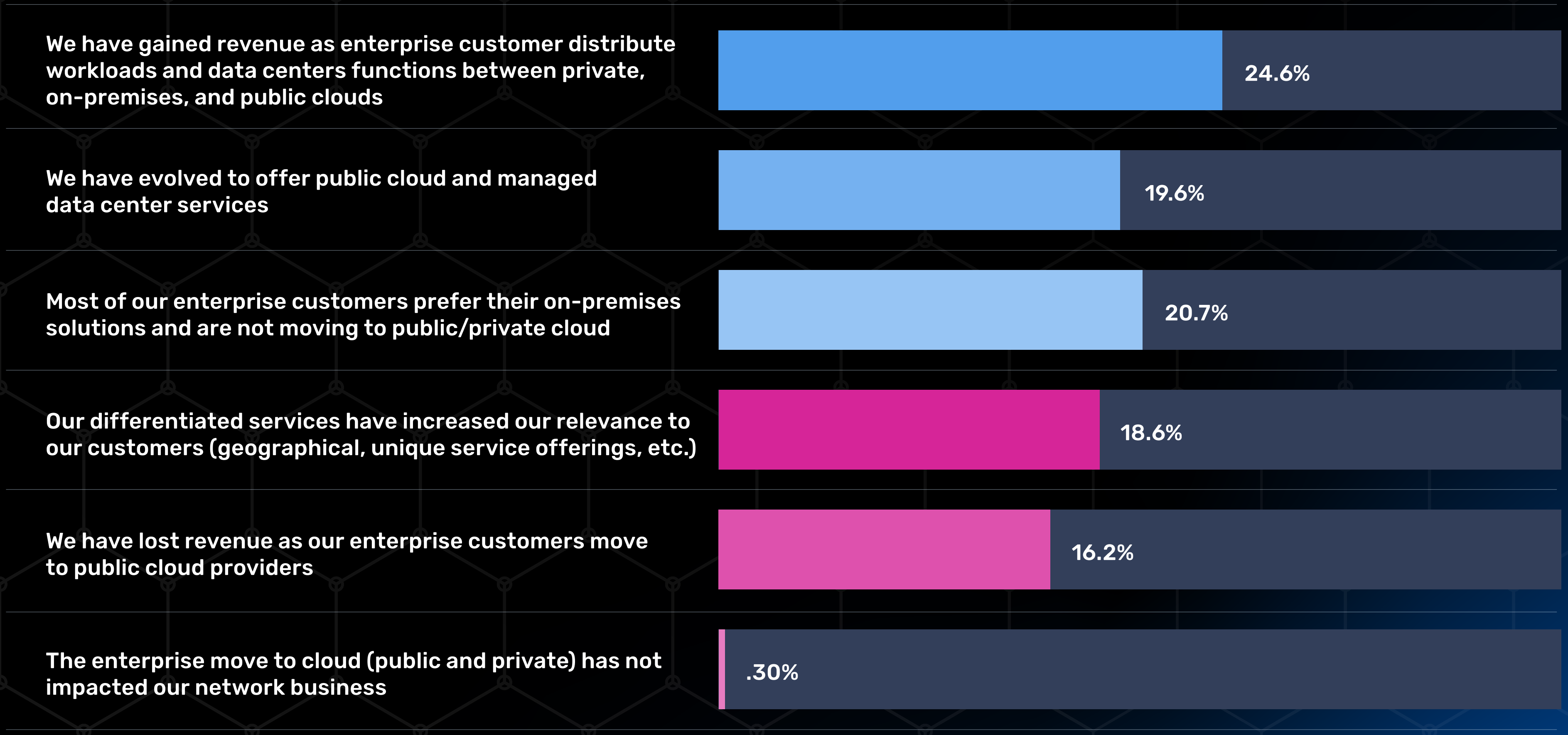
Respondents from Benelux are more likely to be pursuing a strategy of using CGNAT to maximize existing IPv4 allocations, 32 percent compared to a global average of 25 percent.

Almost one-quarter of respondents (23%) said their main approach is to acquire more IPv4 addresses through another service provider, and the same proportion said they would acquire more IPv4 address blocks on the public market. These figures were broadly the same across all geographies.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

Full Survey Results

5. How has the enterprise move to cloud (public and private) impacted your network business, if at all?



4 Top Resiliency Trends

Leveraging Hybrid Cloud Effectively

Continuous Integration and Delivery

Hybrid Cloud Management and Operational Flexibility

Implementing Zero Trust

View eBook

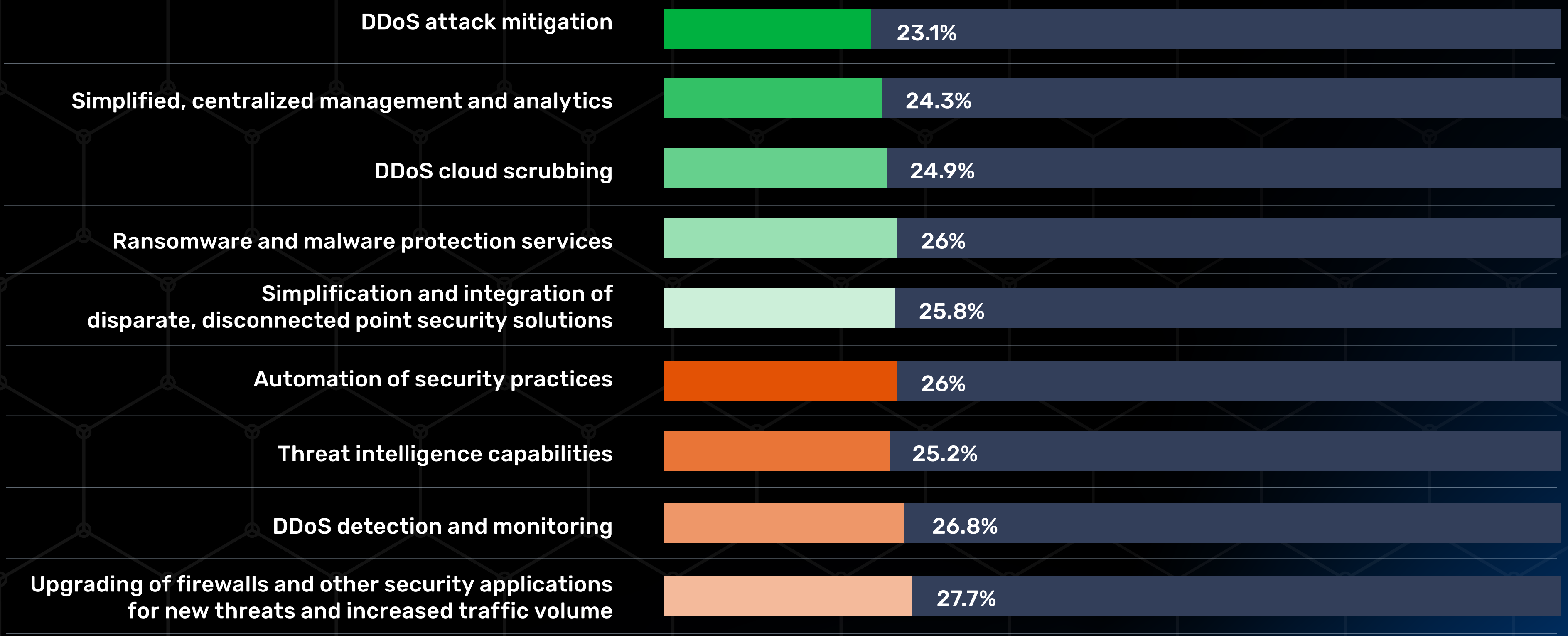
Many respondents say cloud migration has had a positive impact on their organization, whether that is the 25 percent who say it has directly generated revenue, or those who have evolved new public cloud and managed data services (20%) and/or differentiated services to capitalize on cloud migration (19%).

Nevertheless, there remains a solid core of their enterprise customers (21%) that prefer to remain on-premises. This rises to more than 22 percent in the U.S., 23 percent in Benelux and 25 percent in Asia-Pacific and Central and Eastern Europe. On the other hand, it drops to just 15 percent in the Nordic region and 16 percent in Germany.

Sixteen percent of respondents said they had lost revenue as their enterprise customers moved to public cloud providers, though this drops to 12 percent in the UK and rises to 18 percent in the U.S., and 20 percent among Nordics respondents.

Full Survey Results

6. What are your highest priority network security investments for the next 2-3 years, if anything?



There is some variation between the regions over the top network investment priority; those shown here differ from the overall top priority.

Top Priority for Network Investment	Country
Simplification and integration of disparate, disconnected point security solutions	UK
DDoS cloud scrubbing	Southern Europe
DDoS detection and monitoring	Central and Eastern Europe
DDoS attack mitigation	Nordics
Malware and ransomware protection services	Asia-Pacific

While the top priority for network security investment continues to be upgrading firewalls selected by 28 percent, DDoS detection and mitigation (27%) and automation of security policies (26%) followed closely behind. The wide spread of options selected by respondents indicates numerous issues they feel they must cover with network security investment.

In previous A10 Networks research, upgrading firewalls and appliances was the main security investment, but now organizations are indicating a much broader focus, pointing to a more well-rounded strategy overall.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

Full Survey Results

7. What are the top business challenges you see as your networks evolve to new technologies and architecture, if anything?

Challenge	Global respondents selecting it as a key issue	Regions selecting it as their biggest challenge
Increased risk from exposed APIs as a result of app modernization, open source and AI	34.4%	UK, Germany, Nordics,
Supply chain challenges have created shortages that have affected our ability to meet our growth projections	33.7%	U.S., Benelux, Central and Eastern Europe, Asia-Pacific
Growing threats from interconnection and ecosystem partners and IoT devices	32%	India, Southern Europe
Maintaining application availability and security	31.9%	N/A
Maintaining a quality service and avoiding service outages	32.4%	Middle East, Brazil and Mexico
Growing threats of DDoS attacks	28.5%	N/A
Increased competition	27.5%	N/A

A mix of rising risk from emerging technologies and external factors such as supply chain issues, as well as increased interconnection among IT ecosystems lead the challenges, but there are many different issues on the radar, pointing to the complex environment CSPs find themselves in.

Notably supply chain issues to the list for numerous different geographies, indicating the sheer scale of the challenge this has posed for the industry.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

Full Survey Results

8. What are your most important buying criteria for network equipment, if any?

Buying criteria	Total respondents selecting it as a key issue	Regions selecting it as their most important criterion
New network equipment must be in a cloud native form factor	27.8%	UK, U.S., Central and Eastern Europe, Middle East, Germany
Fully integrated with existing operations support systems	26.8%	Asia-Pacific, Benelux
High level of security and availability	26.7%	India, Nordics
Fully automated deployment and maintenance	26%	Brazil and Mexico
New network equipment must be deployable in an edge environment	25.6%	Southern Europe
Compliant with government requirements	25%	N/A
Highest performance	24.4%	N/A
New network equipment must be in a virtual form factor	24.4%	Brazil and Mexico
Lowest price	21.7%	N/A

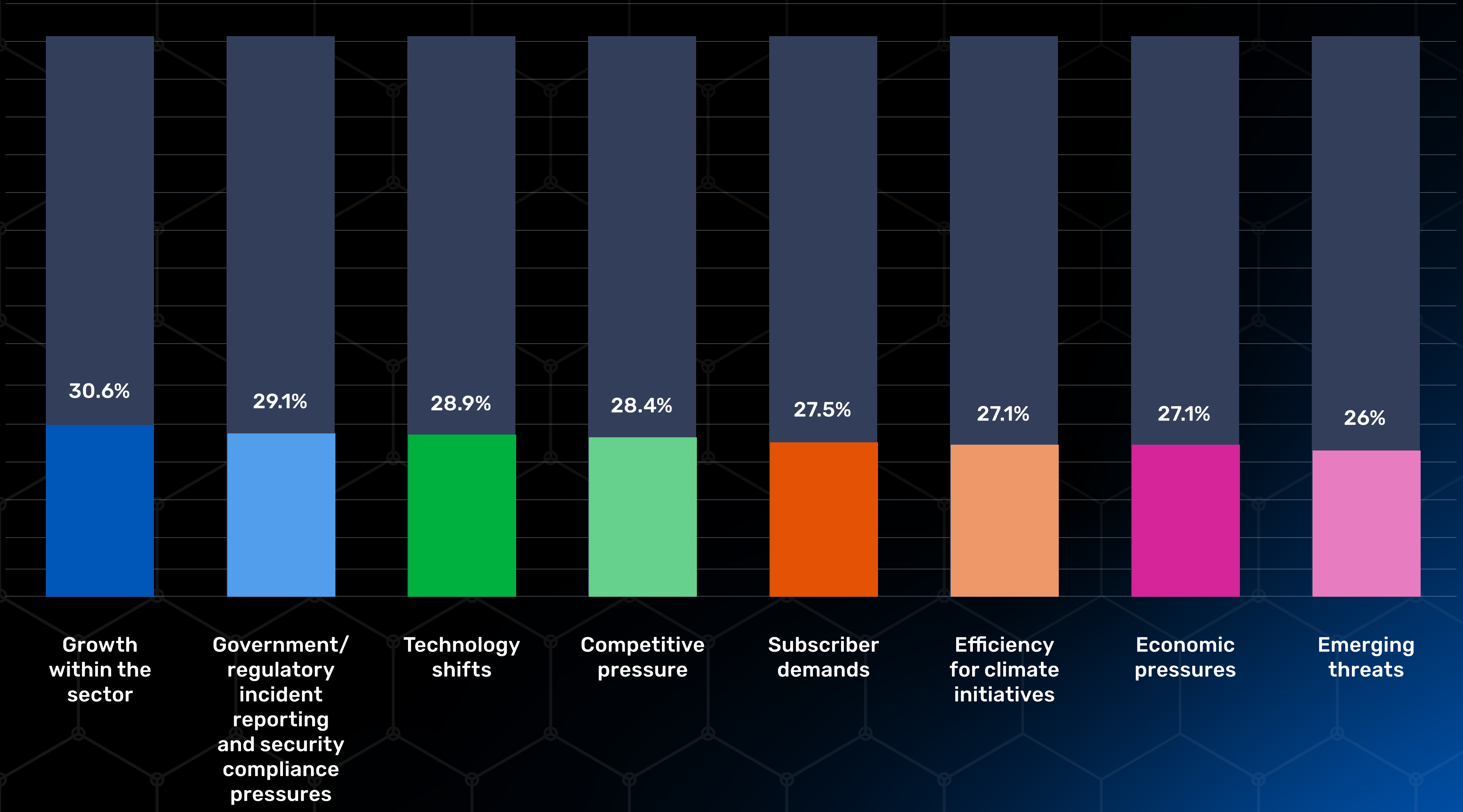
As service providers expand their networks and invest in the future, they have a shopping list of features for the products and services they plan to buy. The list of buying criteria selected by respondents indicates the urgent need to upgrade current networks to make them fit for the future, while also integrating with legacy kit. Asked to select three key decision-making criteria for purchasing network equipment, overall respondents want it to:

- Be in a cloud-native form factor (28%)
- Fully integrate with existing support systems (27%)
- Offer a high level of security and availability (27%)

Regionally, respondents from India and the Nordics were most concerned about having a high level of security and availability, while those from the U.S., UK and Germany are looking for cloud-native form factors. In Benelux and Asia-Pacific, the top criterion is the ability to fully integrate with existing operations support systems.

Twenty-six percent of respondents wanted fully automated deployment and maintenance, while a similar proportion said new equipment must be deployable in an edge environment. Compliance with government requirements was a factor for one-quarter of responses. Twenty-four percent of respondents were seeking high performance and the same number wanted new equipment in a virtual form factor.

9. What is driving you to invest more in network security throughout the organization in the next 2-3 years, if anything?



Overall, growth in the sector is the top motivation for more investment in network security, which makes sense — the more customers and the bigger network you have, the more there is to protect. External pressures from regulators and government compliance requirements are also important, while emerging threats are lower down the list.

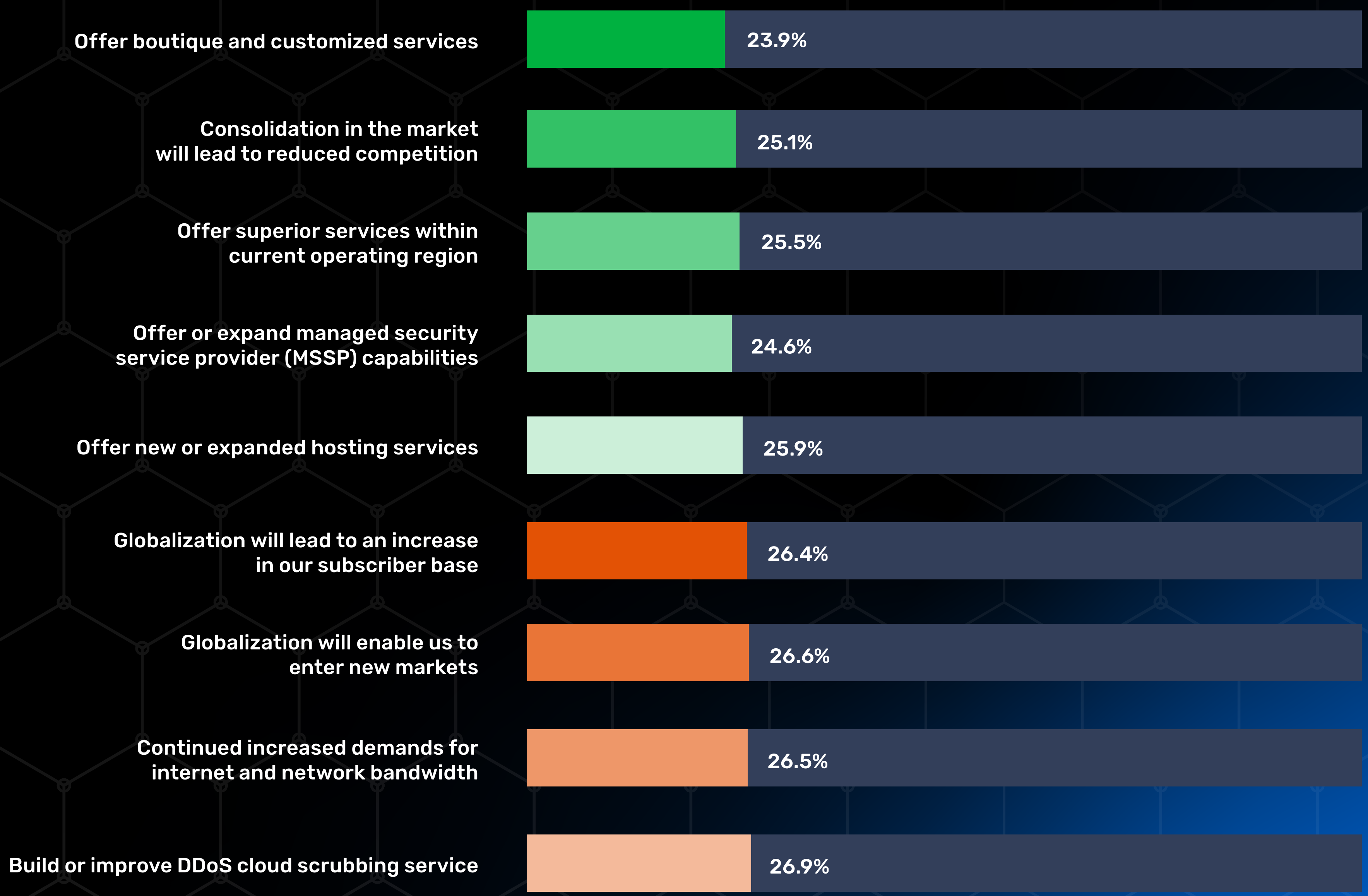
It seems that compliance is driving investment rather more than actual concern about emerging threats. These also sit lower than efficiency for climate initiatives and subscriber demand, indicating that environment, social and governance (ESG) concerns are driving investment more than fears of malicious attacks. This fits much of the current corporate narrative: organizations know that they have a duty to customers and other stakeholders such as investors and regulators, to keep networks secure and available — and they need to be able to demonstrate this to gain clients and investment.

Interestingly, efficiency for climate initiatives was the top factor driving investment in network security in the U.S., ranking second in Germany and Central and Eastern Europe and third in the Nordic region.

Government regulatory reporting and compliance was the top driver in Germany, Nordics, and Central and Eastern Europe.

Full Survey Results

10. What is the biggest business opportunity you see in the next 2-3 years, if anything?



Providers see a lot of opportunity in the market, from general increases in demand and globalization to building new services such as DDoS cloud scrubbing (selected as the top opportunity) and offering expanded services.

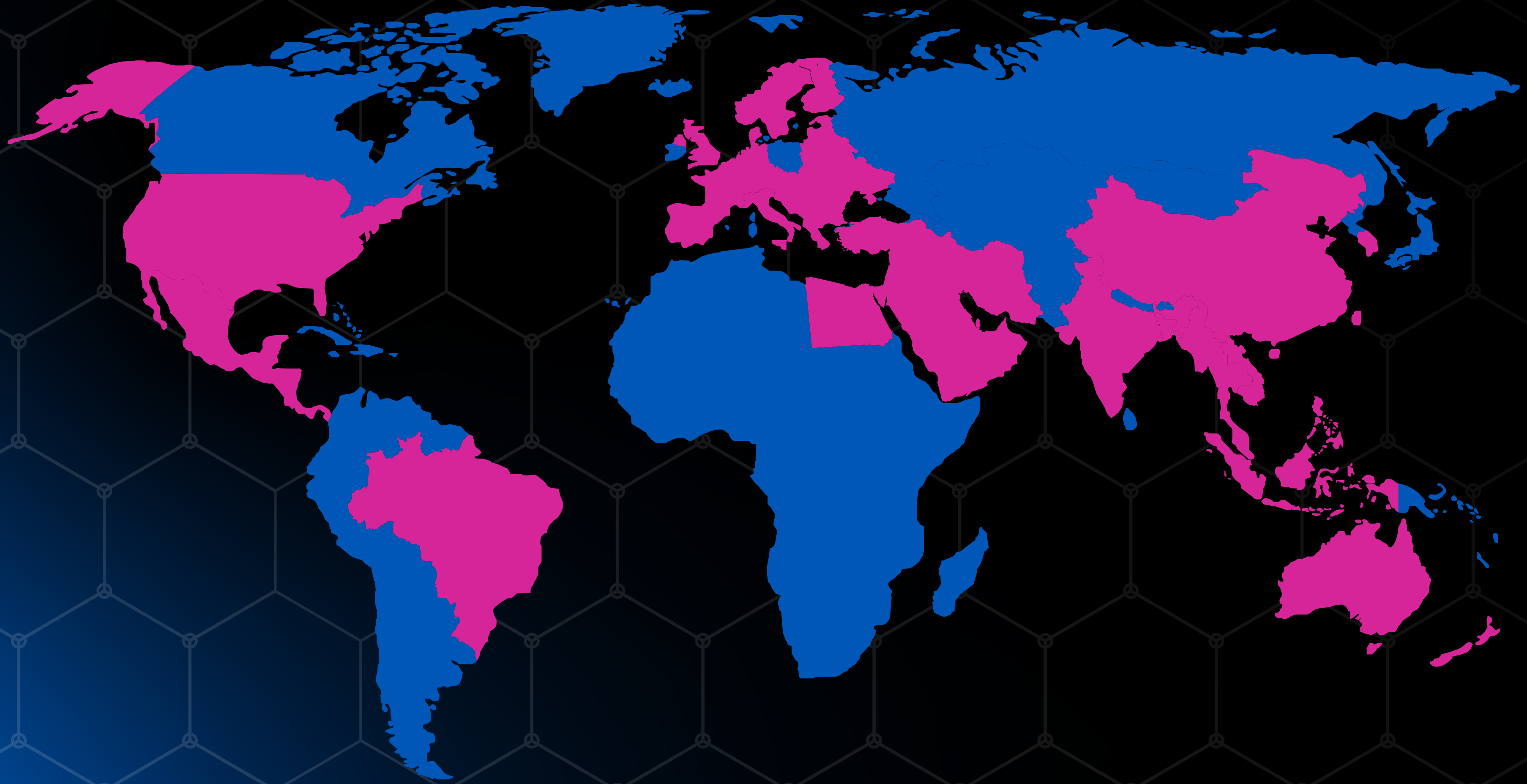
Some regions, such as Asia-Pacific and Brazil and Mexico see market consolidation as an opportunity, while respondents from the Middle East, Benelux, and Central and Eastern Europe see offering new or expanded hosting services as the main advantage on the horizon.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

05.

Regional Analysis

To gain a global perspective on the challenges communication service providers are facing, A10 Networks surveyed senior IT professionals in 21 countries worldwide. These included: United Kingdom, Southern Europe (France and Italy), United States, Germany, India, Middle East (UAE and Saudi Arabia), Benelux (Netherlands and Belgium), Central and Eastern Europe (Hungary, Czech Republic, Poland), Asia-Pacific (Australia, Hong Kong, Singapore), Nordics (Finland, Norway, Sweden), and Brazil and Mexico.



United Kingdom

UK CSPs agree network traffic volumes are only going to trend upwards.

Every UK respondent (100%) expects traffic volumes to increase in the next 2-3 years, and one-quarter (25%) say volumes will soar by between 75-100%. The average increase is expected to be 60%.

The enterprise move to the cloud has positively impacted revenue for 27% of UK CSPs, although there is still a solid core (20%) of enterprise customers who prefer to remain on-premises. Just over one-fifth of UK respondents found that their differentiated services have increased their relevance to customers, while 21% have evolved to offer public cloud and managed data center services.

Looking forward, UK providers see a lot of opportunity in the market from general demand increases to building new services such as DDoS scrubbing. More than a third of UK respondents said globalization will lead to an increased subscriber base and see this as the top opportunity in the future.

100%

say network traffic volumes will increase in the future.

36%

say growth within the sector is the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

30%	Must be in a cloud-native form factor
30%	Must be deployable in an edge environment
29%	Fully integrated with existing systems

UK CSPs selected increased risk from exposed APIs as a result of app modernization, open source and AI as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in the UK

49%	Are expanding their network for an uplift of more than 10% of current subscriber base
14%	Are expanding their network for an uplift of more than 50%
37%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

32%	Simplification and integration of disconnected security solutions
32%	Ransomware and malware protection services
30%	Upgrading of firewalls and other security appliances for new threats and increased traffic volume
28%	Automation of security policies
27%	DDoS detection and monitoring

Southern Europe

Southern Europe CSPs agree network traffic volumes are only going to trend upwards.

Every Southern Europe respondent (100%) expects traffic volumes to increase in the next 2-3 years, and nearly one-fifth (16%) say volumes will soar by between 75-100%. The average increase is expected to be 59%.

The enterprise move to the cloud has positively impacted revenue for 25% of Southern Europe CSPs, although there is still a solid core (20%) of enterprise customers who prefer to remain on-premises. 14% of Southern Europe respondents found that differentiated services have increased their relevance to customers, while 24% have evolved to offer public cloud and managed data center services.

Looking forward, Southern Europe providers see opportunity in the market from general demand increases to building new services such as DDoS cloud scrubbing. More than a quarter of Southern Europe respondents said globalization will enable them to enter new markets and see this as the top opportunity for the future.

100%

say network traffic volumes will increase in the future.

31%

say growth within the sector is the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

27%	Must be deployable in an edge environment
27%	Must also be in a cloud-native form factor
26%	Must have high levels of security and availability

Southern Europe CSPs selected growing threats from interconnection and ecosystem partners and IoT devices as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in Southern Europe

54%	Are expanding their network for an uplift of more than 10% of current subscriber base
19%	Are expanding their network for an uplift of more than 50%
27%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

26%	DDoS cloud scrubbing
26%	Upgrading firewalls and other security appliances
25%	DDoS detection and monitoring
25%	Simplified, centralized management and analytics systems
25%	Automation of security policies

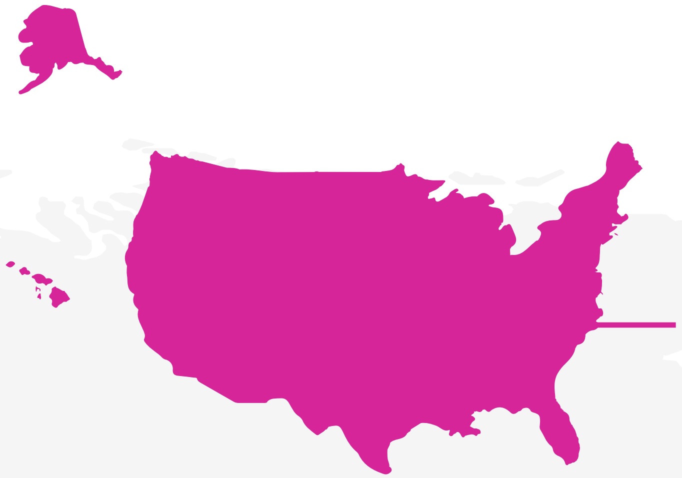
United States of America

U.S. CSPs agree the only way network traffic volumes are going to trend is upwards.

Every U.S. respondent (100%) expects traffic volumes to increase in the next 2-3 years, with 21% saying volumes will soar by between 75-100%. The average increase is expected to be 61%.

The enterprise move to the cloud has positively impacted revenue for 25% of U.S. CSPs, although there is still a solid core (22%) of enterprise customers who prefer to remain on-premises. 22% of U.S. respondents found that their differentiated services have increased their relevance to customers, while 13% have evolved to offer public cloud and managed data center services.

Looking forward, U.S. providers see opportunity in the globalization of the market, leading to an increase in subscribers (28%) with over a quarter (27%) saying that demand for internet and network bandwidth will also increase. They see these as the top opportunities for the future.



100%

say network traffic volumes will increase in the future.

29%

say efficiency for climate initiatives is the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

32%	New network equipment must be in a cloud-native form factor
28%	Must have high levels of security and availability
27%	Must be in a virtual form factor

U.S. CSPs selected supply chain challenges have created shortages that have affected our ability to meet our growth projections as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in the U.S.

54%	Are expanding their network for an uplift of more than 10% of current subscriber base
18%	Are expanding their network for an uplift of more than 50%
28%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

27%	Threat intelligence capabilities
26%	DDoS detection and monitoring
26%	DDoS cloud scrubbing
26%	Simplification and integration of disparate security solutions
25%	Automation of security policies

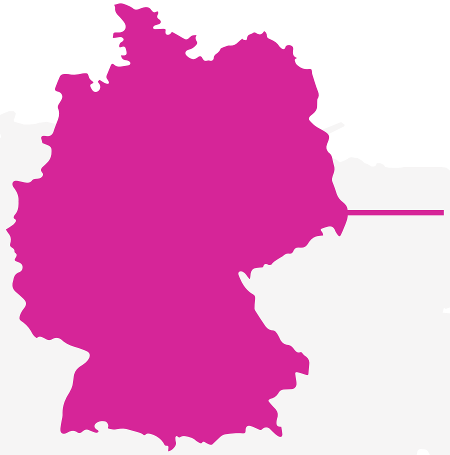
Germany

German CSPs agree the only way network traffic volumes are going to trend is upwards.

99.6% of German respondents expect network traffic volumes to increase in the next 2-3 years, with 12% saying volumes will soar by between 75-100%. The average increase is expected to be 55%.

The enterprise move to the cloud has positively impacted revenue for 24% of German CSPs, although there are still some enterprise customers (16%) who prefer to remain on-premises. 18% of German respondents found that differentiated services have increased their relevance to customers, while 26% have evolved to offer public cloud and managed data center services.

Looking forward, German providers see a lot of opportunity through globalization to enter new markets as well as continued increased demand for internet and network bandwidth. Third on the list of business opportunities was building or improving a DDoS cloud scrubbing service.



99.6%

say network traffic volumes will increase in the future.

33%

say compliance and governance/regulatory reporting pressures are the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

32%	Must be in a cloud-native form factor
30%	Compliance with government requirements
29%	Fully automated deployment and maintenance

German CSPs selected increased risk from exposed APIs as a result of app modernization, open source and AI as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in Germany

46%	Are expanding their network for an uplift of more than 10% of current subscriber base
14%	Are expanding their network for an uplift of more than 50%
40%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

28%	DDoS cloud scrubbing
28%	Upgrading firewalls and security appliances for new threats and increased traffic volumes
28%	Simplification and integration of disparate security solutions
25%	Ransomware and malware protection services

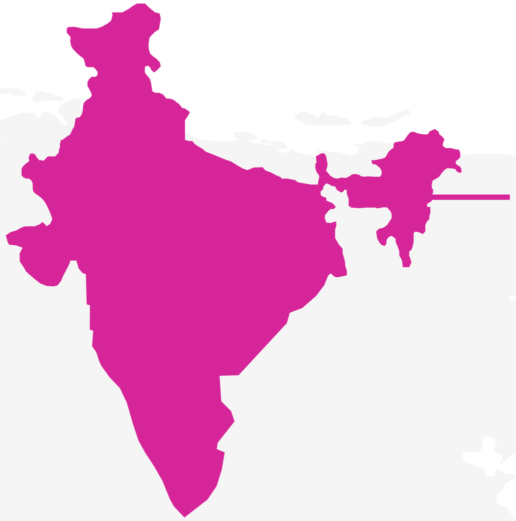
India

Indian CSPs agree network traffic volumes are only going to trend upwards.

Every Indian respondent (100%) expects traffic volumes to increase in the next 2-3 years, and 27% say volumes will soar by between 75-100%. The average increase is expected to be 64%.

The enterprise move to the cloud has positively impacted revenue for 27% of Indian CSPs, although there is still a solid core (21%) of enterprise customers who prefer to remain on-premises. 16% of Indian respondents found that differentiated services have increased their relevance to customers, while 20% have evolved to offer public cloud and managed data center services.

Looking forward, Indian providers see opportunity in the market from increased demand for internet and network bandwidth. More than one-third of respondents (35%) see offering or expanding managed security service provider capabilities as a top opportunity for the future.



100%
say network traffic volumes will increase in the future.

43%
say growth within the sector is the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

37%	Must have high levels of security and availability
36%	Much have fully automated deployment and maintenance
34%	Must fully integrate with operations support systems

Indian CSPs selected growing threats from interconnection and ecosystem partners and IoT devices as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in India

30%	Are expanding their network for an uplift of more than 10% of current subscriber base
11%	Are expanding their network for an uplift of more than 50%
59%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

47%	Upgrading firewalls and other security appliances
37%	Simplification and integration of disparate security solutions
34%	Threat intelligence capabilities
33%	Ransomware and malware protection
33%	DDoS detection and monitoring

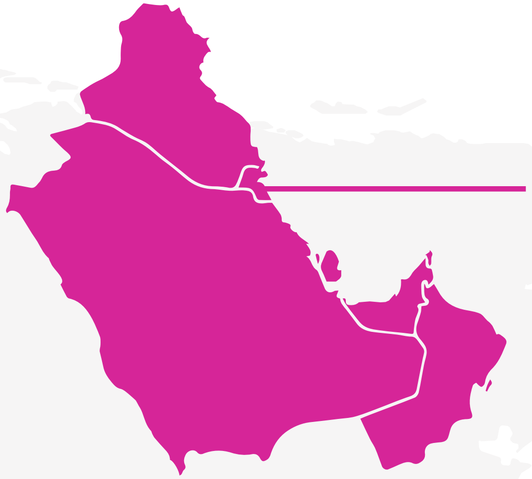
Middle East

Middle East CSPs agree network traffic volumes are only going to trend upwards.

Every respondent (100%) expects traffic volumes to increase in the next 2-3 years, and one in five (20%) saying volumes will soar by between 75-100%. The average increase is expected to be 56%.

The enterprise move to the cloud has positively impacted revenue for 22% of Middle East CSPs, although there is still a solid core (21%) of enterprise customers who prefer to remain on-premises. 18% of Middle East respondents found that differentiated services have increased their relevance to customers, while 19% have evolved to offer public cloud and managed data center services.

Looking forward, Middle East providers see opportunity in the market from general demand increases and globalization to building new services such as DDoS cloud scrubbing. More than a quarter (26%) of Middle East respondents plan to offer new or expanded hosting services, and see this as the top opportunity for the future.



100%

say network traffic volumes will increase in the future.

28%

say growth within the sector is the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

27%	Must be in a cloud-native form factor
27%	Must have the highest performance
26%	Must be compliant with government requirements

Middle East CSPs selected maintaining a quality service and avoiding service outages as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in the Middle East

48%	Are expanding their network for an uplift of more than 10% of current subscriber base
33%	Are expanding their network for an uplift of more than 50%
16%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

25%	Upgrading of firewalls and other security appliances for new threats and increased traffic volume
25%	DDoS detection and monitoring
24%	Ransomware and malware protection services
24%	DDoS cloud scrubbing
24%	Simplified, centralized management and analytics systems

Benelux

Benelux CSPs agree network traffic volumes are only going to trend upwards.

Every respondent (100%) expects traffic volumes to increase in the next 2-3 years, and 16% say volumes will soar by between 75-100%. The average increase is expected to be 58%.

The enterprise move to the cloud has positively impacted revenue for 26% of Benelux CSPs, although there is still a solid core (23%) of enterprise customers who prefer to remain on-premises. 16% of Benelux respondents found that differentiated services have increased their relevance to customers, while 20% have evolved to offer public cloud and managed data center services.

Looking forward, Benelux providers see opportunity in the market, from general demand increases for internet and network bandwidth, to building new services such as DDoS cloud scrubbing. More than a quarter of Benelux respondents plan to offer new or expanded hosting services, seeing this as the top opportunity for the future.

100%

say network traffic volumes will increase in the future.

30%

say technology shifts are the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

30%	Must be fully integrated with existing operations support systems
29%	Must be compliant with government requirements
26%	Must also be in a cloud-native form factor

Benelux CSPs selected supply chain challenges that have created shortages and affected their ability to meet growth projections as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in Benelux

55%	Are expanding their network for an uplift of more than 10% of current subscriber base
18%	Are expanding their network for an uplift of more than 50%
28%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

28%	Ransomware and malware protection services
28%	DDoS detection and monitoring
26%	Automation of security policies
25%	Upgrading firewalls and other security appliances

Central and Eastern Europe

Central and Eastern Europe CSPs agree network traffic volumes are only going to trend upwards.

Every Central and Eastern Europe respondent (100%) expects traffic volumes to increase in the next 2-3 years, and 21% say volumes will soar by between 75-100%. The average increase is expected to be 57%.

The enterprise move to the cloud has positively impacted revenue for 23% of Central and Eastern Europe CSPs, although there is still a solid core (25%) of enterprise customers who prefer to remain on-premises. 22% of Central and Eastern Europe respondents found that differentiated services have increased their relevance to customers, while 14% have evolved to offer public cloud and managed data center services.

Looking forward, Central and Eastern Europe providers see opportunity in the ability to offer new or expanded hosting services (30%) with over a quarter (29%) saying that building or improving DDoS Cloud Scrubbing Services, is also a top opportunity for the future.

100%

say network traffic volumes will increase in the future.

38%

say government/regulatory requirement reporting and security compliance pressures are the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

30%	New network equipment must be in a cloud native form factor
29%	Must be fully integrated with existing operations support systems
28%	New network equipment must be deployable in an edge environment

In Central and Eastern Europe, CSPs noted that supply chain challenges have created shortages that have affected our ability to meet our growth projections as a top business challenge as networks evolve.

Investments to meet the needs of unserved/underserved communities in Central and Eastern Europe

49%	Are expanding their network for an uplift of more than 10% of current subscriber base
18%	Are expanding their network for an uplift of more than 50%
32%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

35%	DDoS detection and monitoring
28%	Threat intelligence capabilities
28%	DDoS cloud scrubbing
28%	Upgrading firewalls and other security appliances

Asia-Pacific

Asia-Pacific CSPs agree network traffic volumes are only going to trend upwards.

Every respondent (100%) expects traffic volumes to increase in the next 2-3 years, and 16% say volumes will soar by between 75-100%. The average increase is expected to be 58%.

The enterprise move to the cloud has positively impacted revenue for 23% of Asia-Pacific CSPs, although there is still a solid core (25%) of enterprise customers who prefer to remain on-premises. 18% of Asia-Pacific respondents found that differentiated services have increased their relevance to customers, while 18% have evolved to offer public cloud and managed data center services.

Looking forward, Asia-Pacific providers see opportunity in consolidation in the market leading to reduced competition. A quarter of Asia-Pacific respondents plan to offer boutique and customized services, seeing this as a top opportunity for the future.

100%

say network traffic volumes will increase in the future.

28%

say subscriber demand is the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

27%	Must be fully integrated with existing operations support systems
26%	Must have a high level of security and availability
25%	Must be the lowest price

Asia-Pacific CSPs selected supply chain challenges that have created shortages and affected their ability to meet growth projections as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in Asia-Pacific

56%	Are expanding their network for an uplift of more than 10% of current subscriber base
18%	Are expanding their network for an uplift of more than 50%
28%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

28%	Ransomware and malware protection services
26%	Simplification and integration of disparate security solutions
25%	Upgrading firewalls and other security appliances
24%	DDoS detection and monitoring

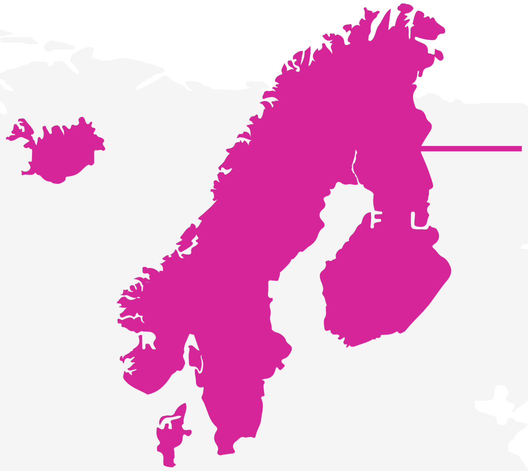
Nordics

Nordics CSPs agree network traffic volumes are only going to trend upwards.

Most respondents (97%) expect traffic volumes to increase in the next 2-3 years, and 13% say volumes will soar by between 75-100%. The average increase is expected to be 55%.

The enterprise move to the cloud has positively impacted revenue for 23% of Nordics CSPs. There is still a solid core (15%) of enterprise customers that prefer to remain on-premises, but fewer compared to other regions, where the figure is around 21%. 20% of Nordics respondents found that differentiated services have increased their relevance to customers, while 22% have evolved to offer public cloud and managed data center services.

Looking forward, Nordics providers see opportunity in the market from building new services such as DDoS cloud scrubbing, and offering or expanding MSSP capabilities. However, one-third of Nordics respondents say the main opportunity is continued increased demand for internet and network bandwidth.



97%

say network traffic volumes will increase in the future.

34%

say government/regulatory incident reporting and security compliance pressures are the top motivation for more investment in network security.

Top-three buying criteria for new network equipment:

32%	Must have high levels of security and availability
29%	Must be fully integrated with existing operations support systems
28%	Must be in a virtual form factor

Nordics CSPs selected increased risk from exposed APIs as a result of app modernization, open source and AI as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in the Nordics

53%	Are expanding their network for an uplift of more than 10% of current subscriber base
18%	Are expanding their network for an uplift of more than 50%
28%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

30%	DDoS attack mitigation
29%	Automation of security policies
29%	DDoS detection and monitoring
27%	Threat intelligence capabilities

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

Brazil and Mexico

Brazil and Mexico CSPs agree network traffic volumes are only going to trend upwards.

All respondents (100%) expect traffic volumes to increase in the next 2-3 years, and 15% say volumes will soar by between 75-100%. The average increase is expected to be 59%.

The enterprise move to the cloud has positively impacted revenue for 27% of Brazil and Mexico CSPs. There is still a solid core (19%) whose enterprise customers prefer to remain on-premises. 20% of Brazil and Mexico respondents found that differentiated services have increased their relevance to customers, while 19% have evolved to offer public cloud and managed data center services.

Looking forward, Brazil and Mexico providers see opportunity from offering superior services within their region. 28% of Brazil and Mexico respondents say a top opportunity is market consolidation which will lead to reduced competition.

100%

say network traffic volumes will increase in the future.

30%

say competitive pressure and economic pressure are equal top motivations for more investment in network security.

Top-three buying criteria for new network equipment:

26%	Must be in a virtual form factor
24%	Must have fully automated deployment and maintenance
24%	Must be deployable in an edge environment

Brazil and Mexico CSPs selected maintaining a quality service and avoiding service outages as a top business challenge as networks evolve.

Investments to meet the needs of unserved/ underserved communities in Brazil and Mexico

56%	Are expanding their network for an uplift of more than 10% of current subscriber base
28%	Are expanding their network for an uplift of more than 50%
26%	Are building out additional data centers and capacity for other CSPs

Highest priority network security investments in the next 2-3 years

26%	Automation of security policies
23%	DDoS cloud scrubbing
23%	Upgrading firewalls and security appliances for new threats and increased traffic volumes
23%	Simplified, centralized management and analytics systems

06.

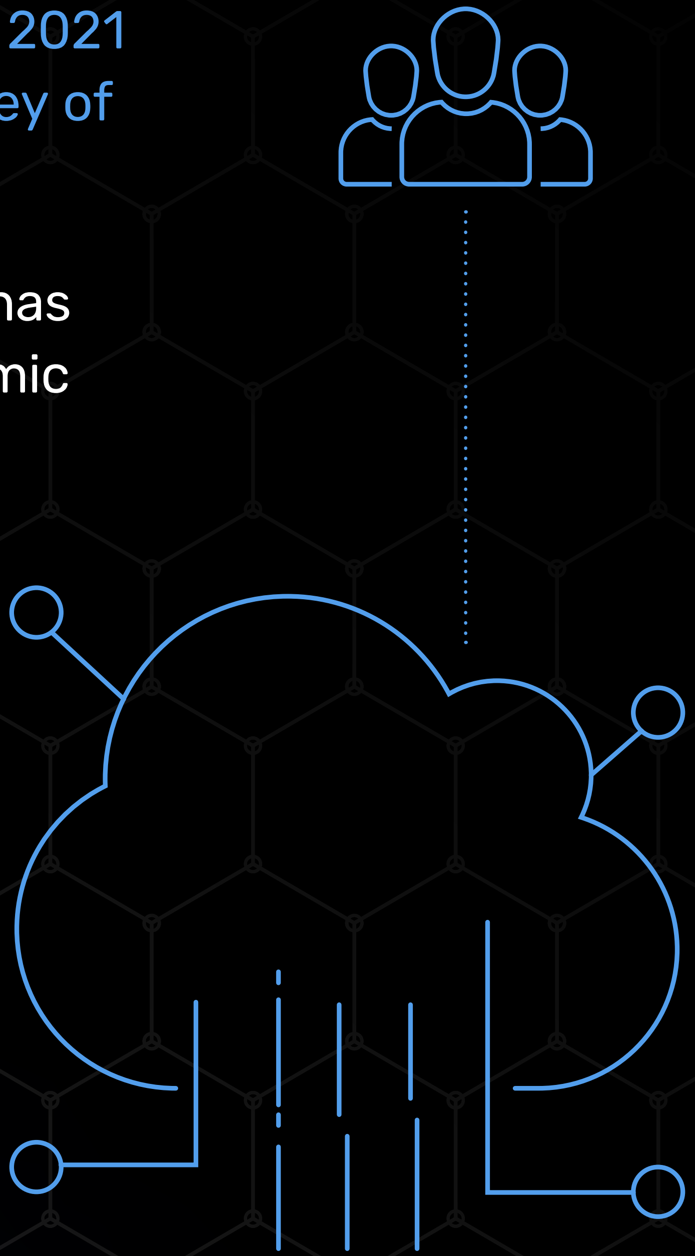
Looking Back, Looking Forward: 2021 to 2023 Comparisons

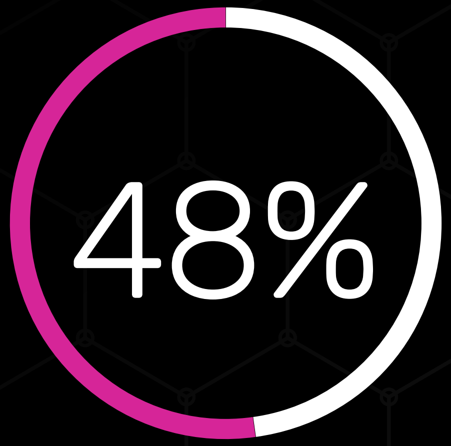
The world is in a very different place than in 2021 when A10 Networks conducted its first survey of communication service providers.

In 2023, the pandemic is largely over, but it has been superseded by geopolitical and economic uncertainty on an equally global scale.

Recovery looks to be challenging.

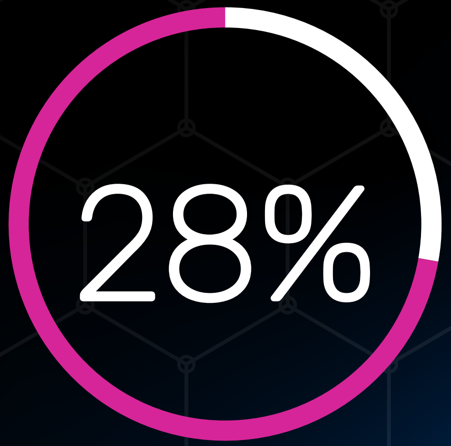
Undoubtedly, connectivity played a vital role in keeping the wheels of society and business turning during the pandemic, and it is equally essential during today's uncertainty. As such, there are some areas where of comparison between the responses from the 2021 survey, and those received in 2023.





In 2021 respondents top priority was upgrading firewalls and other security appliances.

↓



In 2023 prioritizing firewalls had dropped to 28% and DDoS detection, monitoring, and automation of security policies were viewed as almost equally important.

The COVID Surge has Passed, but Expectations Around Traffic Growth Remain High

In early 2021, 99 percent of respondents reported that traffic had surged as a result of COVID-19, on average by 55 percent over the year since lockdowns began. Now, the surveyed professionals predict that a similar level of traffic increase (58%) will occur over the next two to three years. This indicates that they expect traffic growth to continue.

Investment Plans are Back on Track

Understandably, the pandemic caused some CSPs to adopt a cautious approach to investment. In 2021, 49 percent said they had put investment plans on hold, although investment in security remained a priority in light of the increasing threats faced. In 2023, despite continuing uncertainty, investment is looking strong in areas from expanding networks to reach unserved/underserved communities, to network security. Indeed, all but two respondents are investing in network security in the coming two to three years.

Maintaining Reliable Services Remains Essential

Maintaining quality service and avoiding outages were among the top-three business challenges perceived by this year's survey respondents. This aligns with their sentiment from the 2021 survey, where eliminating service disruption and downtime were priorities.

DDoS Detection and Monitoring is Rising as an Investment Area

In 2021, the highest investment priority was upgrading firewalls and other security appliances for new threats and increased traffic volume. Almost half (48%) of respondents felt this was their top priority, far ahead of any other activity. This time, when asked a similar question, the percentage prioritizing firewalls had dropped to 28 percent and other investments such as DDoS detection and monitoring, DDoS cloud scrubbing, and automation of security policies were viewed as almost equally important. It seems that CSPs are now looking to build more sophisticated defense-in-depth security strategies bringing in a broader range of tactics as they build out networks for the future.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

07.

Reflections and Recommendations

The global research shows that communication service providers are at a crucial point as they aim to capitalize on demand and seize opportunities to grow and diversify their businesses.

To realize the market's full potential, service providers need to scale their networks while protecting them, so the infrastructure they provide is secure and highly available. This is essential if they are to effectively manage the increase in subscribers, devices, and applications that are underway.

A10 Networks Recommends:

- ✓ **Work with security partners to scale networks safely** and supersede legacy systems with the deployment of AI, machine learning, and threat intelligence capabilities that are a match for the threat levels experienced in growing networks.
- ✓ **Leverage automation** to simplify management, improve control over network resources and guarantee uptime while gaining full visibility into all network traffic.
- ✓ **Support future subscriber and IoT growth** by implementing a full IPv4 to IPv6 migration plan, with interim IPv4 preservation through carrier-grade NAT (CGNAT).
- ✓ **Regional providers should explore the potential of advanced core technologies,** public/private partner models, and opportunities to offer adjacent cybersecurity and managed IT services to overcome the challenges of building out networks to unserved/underserved communities.

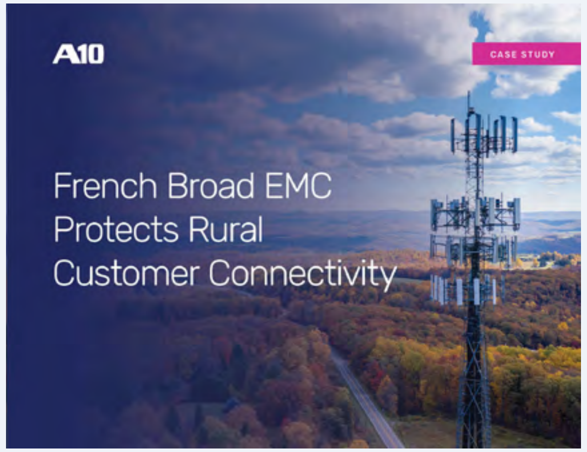
For further insights from A10 Networks, and to learn how our solutions can address the myriad of challenges facing communication service providers today, please download the following resources:

A10

EBOOK

Dodging and Defeating DDoS Attacks:
Data Center Provider Guide

▶ Dodging and Defeating DDoS Attacks: Data Center Provider Guide


A10

CASE STUDY

French Broad EMC Protects Rural Customer Connectivity

▶ French Broad EMC Protects Rural Customer Connectivity

Or visit the A10 resource hub at A10networks.com/resources/ for deployment guides, case studies, data sheets, and more.

Introduction
Methodology
Executive Summary
Top Findings
Regional Analysis
Comparisons
Next Steps
About A10

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-14161-EN-01 APRIL 2023