

The ROI of QoE

Get the most out of your deployed network

Telco Smart Trends Report H1 2023



Table of Contents

QoE is More Complicated than QoS	3
It's a Data-driven World	4
Quality = Money	4
If You Can't Measure It, it's Hard to Improve It	5
Network Expansion is a Costly Solution to Low QoE	6
DDoS – The Silent QoE Killer	7
Is 5G the QoE Silver Bullet?	8
Smart QoE Management & Automated DDoS Mitigation	9
Key Takeaways	11
Methodologies	12
Resources	13

QoE Is More Complicated than QoS

QoS (Quality of Service) and QoE (Quality of Experience) are two key metrics that Communications Service Providers (CSPs) use to monitor the performance of their services. While QoS measures the technical performance of the network, such as latency, bandwidth, and packet loss, QoE reflects the end-user's perception of the service quality.

At the end of the day, QoE is more important because it reflects the end-user's experience. Technical measurements may be fine, yet our experience might be unsatisfactory. You and I don't really care about QoS measurements as long as our video flows, our sports are immersive, our music is high fidelity, and our AR/VR is realistic. We'd also like our e-health to be timely and our autonomous vehicles to be safe.

But QoE is more complicated to measure than QoS. By nature, quality of experience is subjective; it's also multi-dimensional, must be captured in real-time in order to impact it, and it lacks standardized measurement methodologies.

QoE also has significant business implications. Broadband markets tend to be highly saturated and CSPs cannot afford to lose subscribers for any reason, let alone poor QoE. In addition, as CSPs shift limited resources to 5G, they need their 4G networks to work well, automatically, and without requiring expensive reconfiguring or expansion.

In today's competitive landscape, **CSPs need advanced analytics, monitoring, and management tools** to continuously measure and improve the QoE of their services.

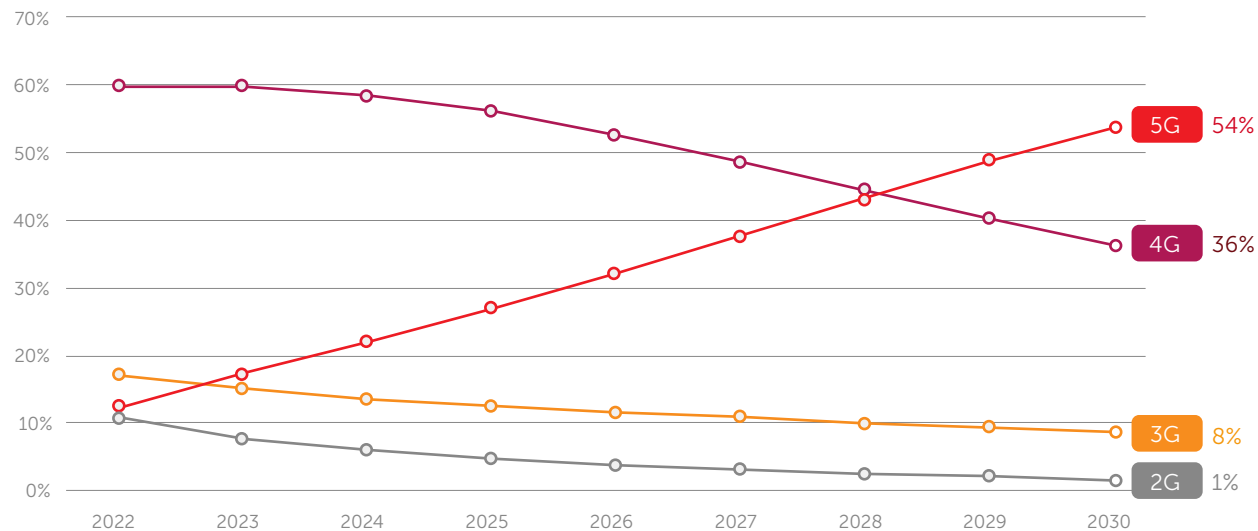
To understand how CSPs currently view QoE as both a challenge and an opportunity, we recently collaborated with Coleman Parkes Research to conduct a worldwide, anonymous survey of Tier-1 and Tier-2 mobile network operators, half of whom were also fixed network operators. The results of this survey are presented in this Allot Telco Smart Trends report.



It's a Data-driven World

According to the recent GSMA "THE MOBILE ECONOMY 2023" report, "Mobile penetration is approaching saturation in most markets around the world, especially among adult and urban populations" with "5.4 billion unique mobile subscribers in 2022." While there is a lot of hype around the rapid deployment of 5G networks, 4G is still the dominant mobile network technology around the world. GSMA further reports that "Mobile traffic growth is driven by a combination of factors, including video streaming and online gaming. Video traffic is estimated to account for around 70% of all mobile data traffic" and 80% of overall Internet traffic

Mobile adoption by technology
Percentage of total connections



Quality = Money

We asked CSPs if they thought they could make more money by guaranteeing QoE. They responded that they could charge 10% more, on average, to those customers who were interested in this kind of SLA. 39% responded that the surcharge could be as high as 15% and another 12% said it could be even higher. 60% felt this was relevant for between 6-10% of their customer base.

Assuming a network of 10 million users, paying 10 Euros per month, **this would yield an extra 8.4 million Euros annually**, from an existing customer base.

Presumably, customer satisfaction would be higher, and the brand reputation would also improve, yielding additional financial benefits.

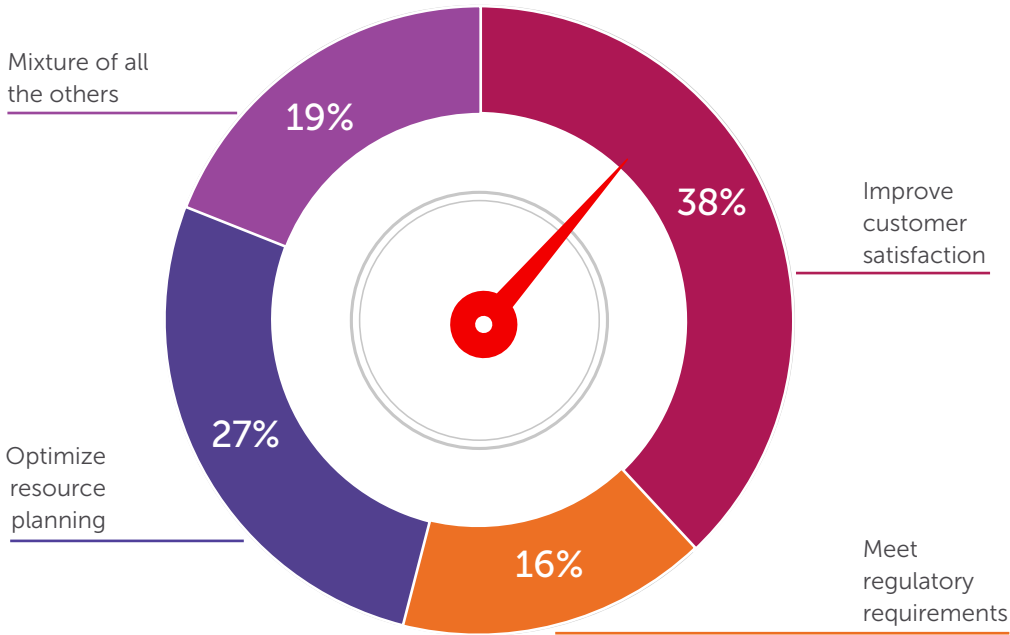


On average,
7% of
customers
would spend
10% more
for a guaranteed QoE SLA

If You Can't Measure It, It's Hard to Improve It

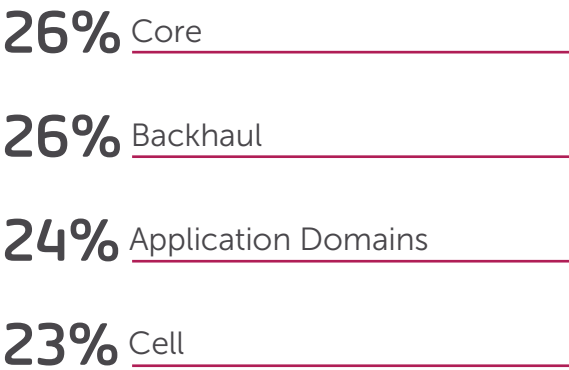
When asked to explain the primary objective of measuring QoE, nearly 40% of CSPs said it was to improve customer satisfaction, and that reaches nearly 50% in Tier-1 CSPs. The 2nd leading objective was to optimize resource planning.

Primary objective of measuring QoE

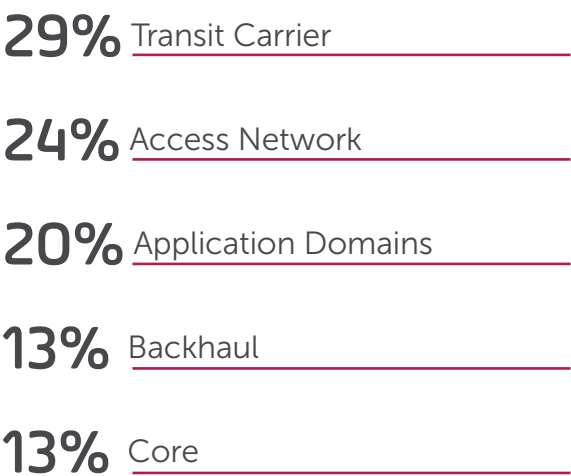


Network Segment Most Impacted by Congestion

Mobile Networks



Fixed Networks



Network congestion is one of the main causes of poor QoE. If networks don't have enough capacity to ensure the quality of all their services all of the time, QoE will suffer. Given the clear understanding of why QoE should be measured, it was somewhat surprising to learn that **23% of CSPs do not have a tool for monitoring network congestion**. Less surprising, but still problematic, was the finding that **28% of CSPs lack tools to improve QoE in real-time**. For these CSPs, guaranteed QoE and optimal resource planning are out of reach. They have neither the data nor the tools to make this possible.

This was particularly surprising given that, through the survey, CSPs reported that all sections of their mobile network are, more or less, equally impacted by network congestion.

Fixed networks also have congestion issues, particularly in the transit carrier and access sections of the network. Here too, QoE should be measured, and real-time tools should be used to assure that performance-sensitive applications are prioritized over less sensitive and background traffic.

Network Expansion is a Costly Solution to Low QoE

The easiest solution to congestion is increased capacity. Sometimes you have to add capacity to keep up with traffic growth and, in fact, 76% of CSPs make investments in network capacity expansion at least every 2-3 years. On average, 12% of mobile cells require capacity upgrades every year. The average cost per cell capacity upgrade was reported to be \$14,000. Assuming a network of 60,000 cells, this is quite an expensive proposition. A similar calculation can be made for fixed networks..

$$\begin{array}{ccccc} \text{60k} & \times & \text{12\%} & \times & \text{\$14k} & = & \text{\$100m} \\ \text{Cells} & & \text{Capacity} & & \text{Average cost} & & \\ & & \text{upgrades} & & \text{per cell capacity} & & \\ & & & & \text{upgrade} & & \end{array}$$

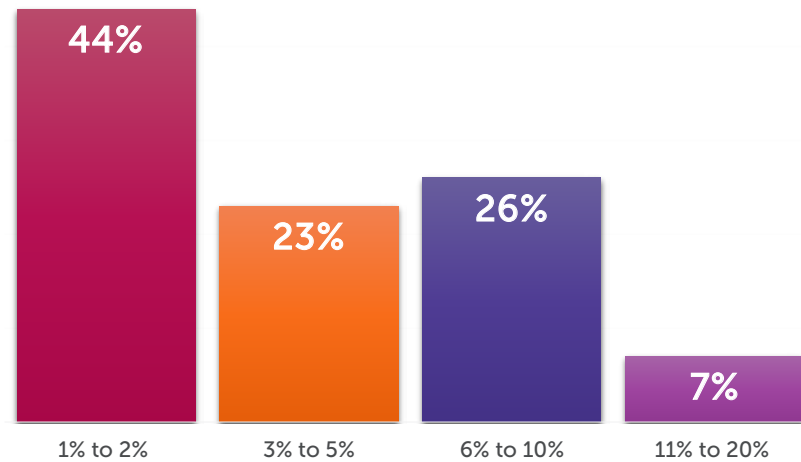
If it were possible to overcome some degree of congestion without resorting to capacity expansion, significant savings would accrue.



DDoS – The Silent QoE Killer

Distributed Denial of Service (DDoS) attacks are a well-known and continuously growing fact of worldwide telecommunications networks. The growing DDoS threat recently prompted the US Cybersecurity and Infrastructure Security Agency (CISA), in conjunction with the FBI and other organizations, to update guidelines to reduce the likelihood and impact of DDoS attacks.

Numerous INDUSTRY REPORTS indicate that CSPs are increasingly targets of the largest DDoS attacks. Even when not the direct target of an attack, there is the added background impact on CSPs, because they serve as the conduit of attacks aimed at their customers



CSPs believe, on average, that **5%** of network capacity is always being taken up by DDoS traffic.

33% believe it is higher.

Allot's experience around the world indicates that this is closer to **10%**.

DDoS steals **5-10%** of network capacity, on average.

Automated mitigation would therefore reduce the need for capacity expansion by **\$5-10M, annually**

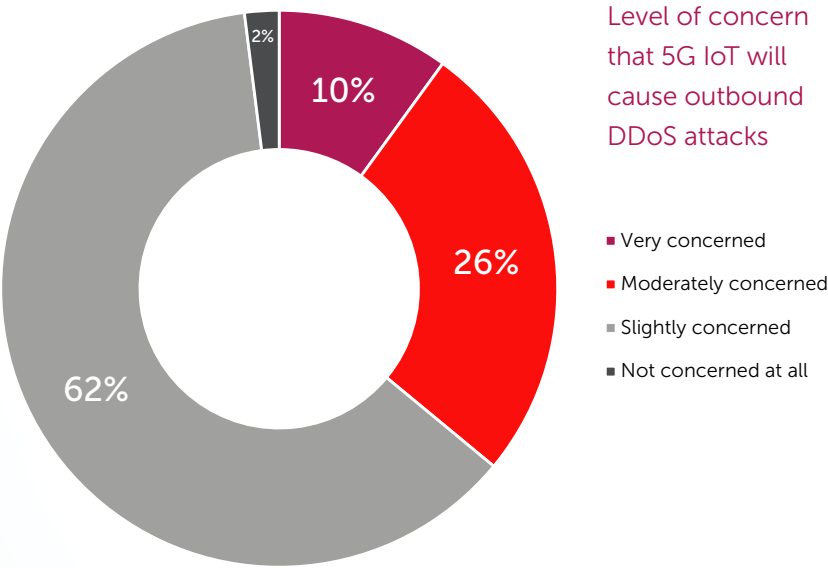
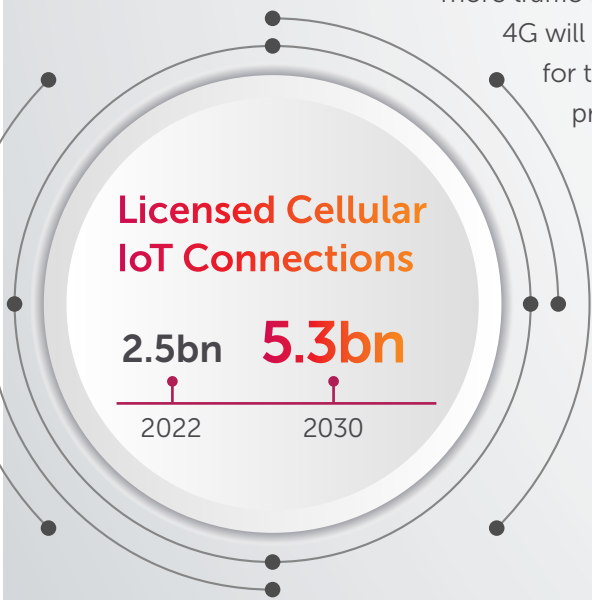
Allot has demonstrated the ability to recover this amount of bandwidth through its DDoS Secure and 5G NetProtect automated DDoS mitigation solutions. If we apply these figures to the network expansion costs in the previous example, then we see that automated mitigation could reduce the need for capacity expansion by \$5-10 million annually.



Is 5G the QoE Silver Bullet?

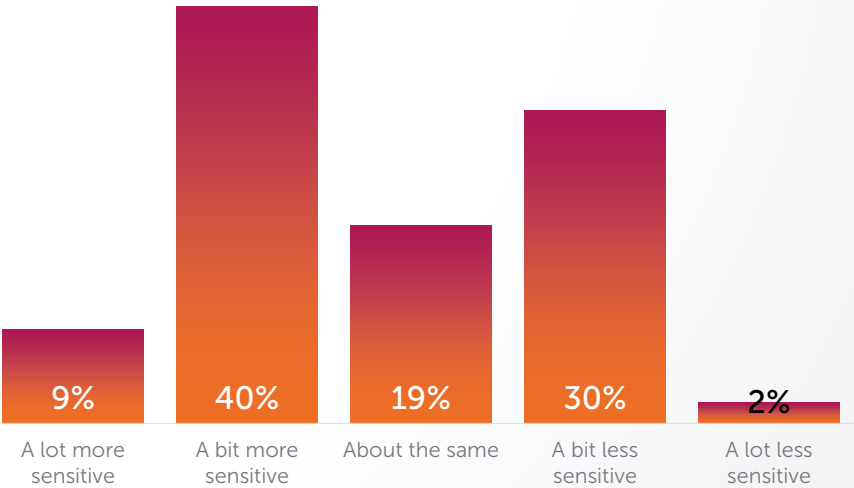
It is tempting to think that 5G will solve all the QoE concerns for CSPs. Perhaps the enhanced, massive broadband that's promised will simply outstrip congestion issues and will provide enough capacity for everyone's needs. Dedicated slices sound like the solution for guaranteed SLAs, even for special cases requiring ultra-low latency. 73% of our survey respondents believe 5G will improve congestion.

While 5G will undoubtedly help, **every technology has eventually confronted capacity limitations**. Like the automobile industry has shown, induced demand is real -- the more capacity you create, the more traffic that is generated. In addition, 4G will continue to dominate traffic for the next 5 years (as seen in the previously cited GSMA report, by number of connections), and CSPs need ways to minimize 4G spending.



The third pillar of 5G is Massive Machine Type Communications – IoT. An explosion of connected devices is anticipated. According to the GSMA report cited earlier, this should grow from 2.5 to 5.3bn devices in the coming 7 years. Already, **36% of our respondents are moderately or very concerned** that IoT traffic could generate outbound DDoS attacks, appearing to originate from their networks.

In addition to degrading traffic and performance-sensitive services, outbound DDoS attacks will undoubtedly damage the CSP's reputation as well. 5G networks are designed with a distributed architecture, featuring multi-access edge connection points (MECs), which further increases the threat attack landscape. This, along with the anticipated proliferation of poorly secured IoT devices, perhaps explains why our survey respondents were concerned about 5G vulnerability to DDoS attacks.



Smart QoE Management & Automated DDoS Mitigation

Smart QoE Management

From our experience with multiple CSPs around the world, we have seen how advanced QoE management can turn potentially service-affecting congestion into managed traffic with acceptable QoE. This requires sophisticated application awareness and the ability to prioritize performance-sensitive services in real time. Consistent with our surveys from 2019 and 2021, 62% of CSPs agree that industry regulations allow services to be prioritized.

62% Services

58% Applications

56% Users

51% Service Plans

Allot traffic management solutions offer a multi-pronged approach to congestion management, with three different offerings to ensure satisfactory QoE.



Static - Time of Day
Fixed/Mobile

Application aware prioritization, for use-cases where peak-hours are well known and static



Closed Loop Automation
Fixed

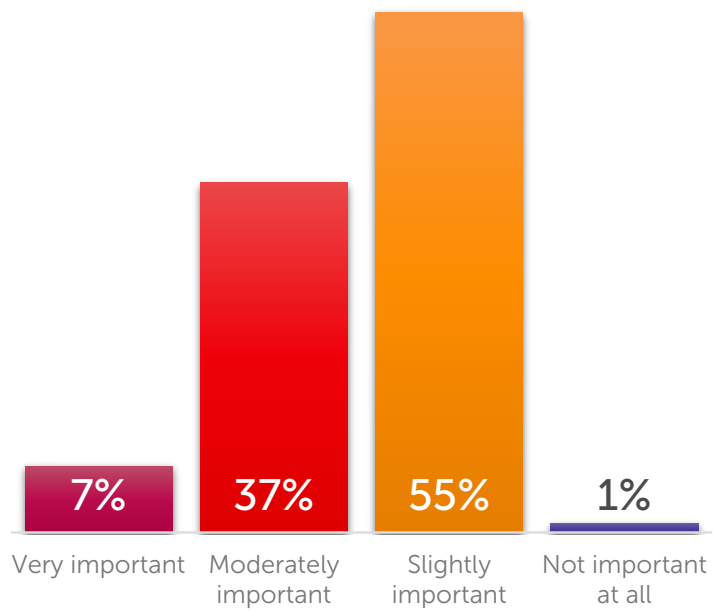
Congestion detection thresholds, based on RTT metrics



Bearer Management
Mobile

Application aware scheduling of dedicated bearers

Allot has demonstrated the ability to add as much as 15% usable capacity to seemingly congested networks.



The importance of dynamic prioritization during an attack

Automated DDoS Mitigation

Rapid mitigation of volumetric DDoS attacks is critical for CSPs to maintain service availability. It will become even more critical as ultra-low latency 5G services are rolled out because they will not be able to tolerate congestion-induced latency.

Often overlooked in DDoS solutions is the need to prioritize specific applications and services during early stages of attack, detection, and mitigation. Happily, CSPs appear to understand this. Fully 99% indicated that this is important, with 44% calling it moderately or very important.

Allot's DDoS mitigation solutions can reclaim the 5-10% of network traffic "stolen" by DDoS attack activity, while dynamically ensuring capacity during attack/mitigation. On 4G networks, Allot DDoS Secure detects and mitigates even zero-day volumetric attacks within approximately 5 seconds, thanks to machine learning that benchmarks normal traffic pattern to speed up recognition of anomalous data attack patterns. In conjunction with application-aware traffic management, this ensures that performance-sensitive applications are prioritized during detection and mitigation stages of the DDoS attack. For 5G networks, Allot's 5G NetProtect solution combines the same rapid DDoS detection and mitigation with application-aware prioritization of performance-sensitive applications to ensure QoE during attacks. There is also an optional integration with a leading next-gen firewall to further protect the 5G network from malicious attacks.

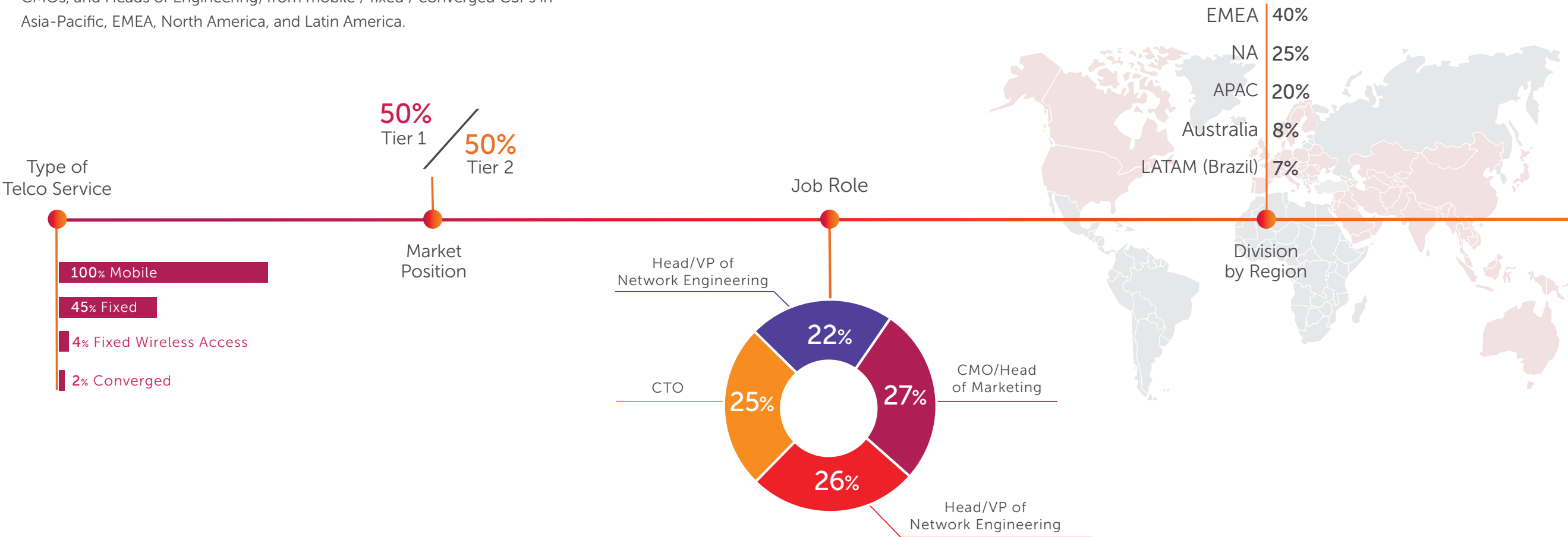




Methodology

During Decembr 2022, COLEMAN PARKES RESEARCH UK conducted an anonymous research project on behalf of Allot. 100 Tier-1 and Tier-2 CSPs, covering mobile, fixed, converged, and FWA networks were surveyed.

A survey was conducted among 100 senior decision makers (CTOs, CNOs, CMOs, and Heads of Engineering) from mobile / fixed / converged CSPs in Asia-Pacific, EMEA, North America, and Latin America.



Resources

In addition to first-hand research conducted within the framework of the December 2022 QoE/DDoS survey, the following resources are of interest for this report:



Dawn of the 5G Era
FROST & SULLIVAN
[Learn more >](#)



The importance of QoE for CSPs
[Learn more >](#)



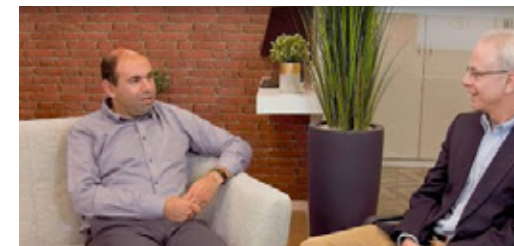
Quality of Experience and its impact on profitability
[Listen now >](#)



Joint CISA FBI MS-ISAC Guide on Responding to DDoS Attacks and DDoS Guidance for Federal Agencies
[Learn more >](#)



Allot Traffic Management Solutions
[Learn more >](#)



From Network KPIs to Customer QoE
[Watch now >](#)

About Allot

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-based security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry-leading network-based security as a service solution is already used by over 20 million subscribers globally. For more information, visit www.allot.com or [Contact Us](#)

