allot

See. Control. Secure.

Closed Loop Automation:

What CSPs Need to Know Now and for the Future

Telco Smart Trends Report, Q1 2019

CLA Is No Longer Just a “Nice to Have”

Automation has long been prevalent in CSP operations, like in OSS root cause analysis, service provisioning or self-optimizing networks. But, with the telecom industry finally on the cusp of large-scale SDN/NFV implementations, and the emergence of 5G networks, Closed Loop Automation (CLA) has become a strategic imperative. CLA will enable CSPs to keep delivering Quality of Experience (QoE) to their subscribers on what promises to be a more complex network, with greater traffic congestion and an increased threat landscape.

The following pages provide mission critical information and insights that will enable you to benchmark your current CLA activity and help pinpoint areas where CLA can improve QoE and drive cost reductions and efficiencies in the future.

We surveyed 100 CSPs worldwide and asked them several questions about the importance of CLA today.

For more details on the survey methodology »

Table of Contents

Yesterday

A Look Back

For years, when Communication Service Providers (CSPs) talked about Closed Loop Automation (CLA), they saw it as a better, more efficient way to solve well-known, well-defined problems. For example, everyone agreed it would be great if OSS Fault Management systems could automatically analyze tens of thousands of alarms to identify the root cause that represented the underlying problem. Clearly, this would be faster than human analysis and mean-time-to-resolution (MTTR) would be greatly reduced. These kinds of solutions have been very successful.

Recently, with the move to Software Defined Networking (SDN) and Network Function Virtualization (NFV), CLA has begun to address dynamic, unpredictable scenarios. Fueled by the need to keep CAPEX and OPEX in check, CSPs have been eager to find ways to avoid worst-case (over) provisioning by responding effectively and efficiently to changing resource demands. SDN and NFV are beginning to do just that.

And Ahead

But with our industry heading towards 5G, how do CSPs perceive the value of CLA as they embark on the transition towards full adoption? Do they think 5G has enough built-in CLA to handle the 'unknown unknowns' around massive, mission critical IoT, enhanced mobile broadband and related large-scale security threats?

Today

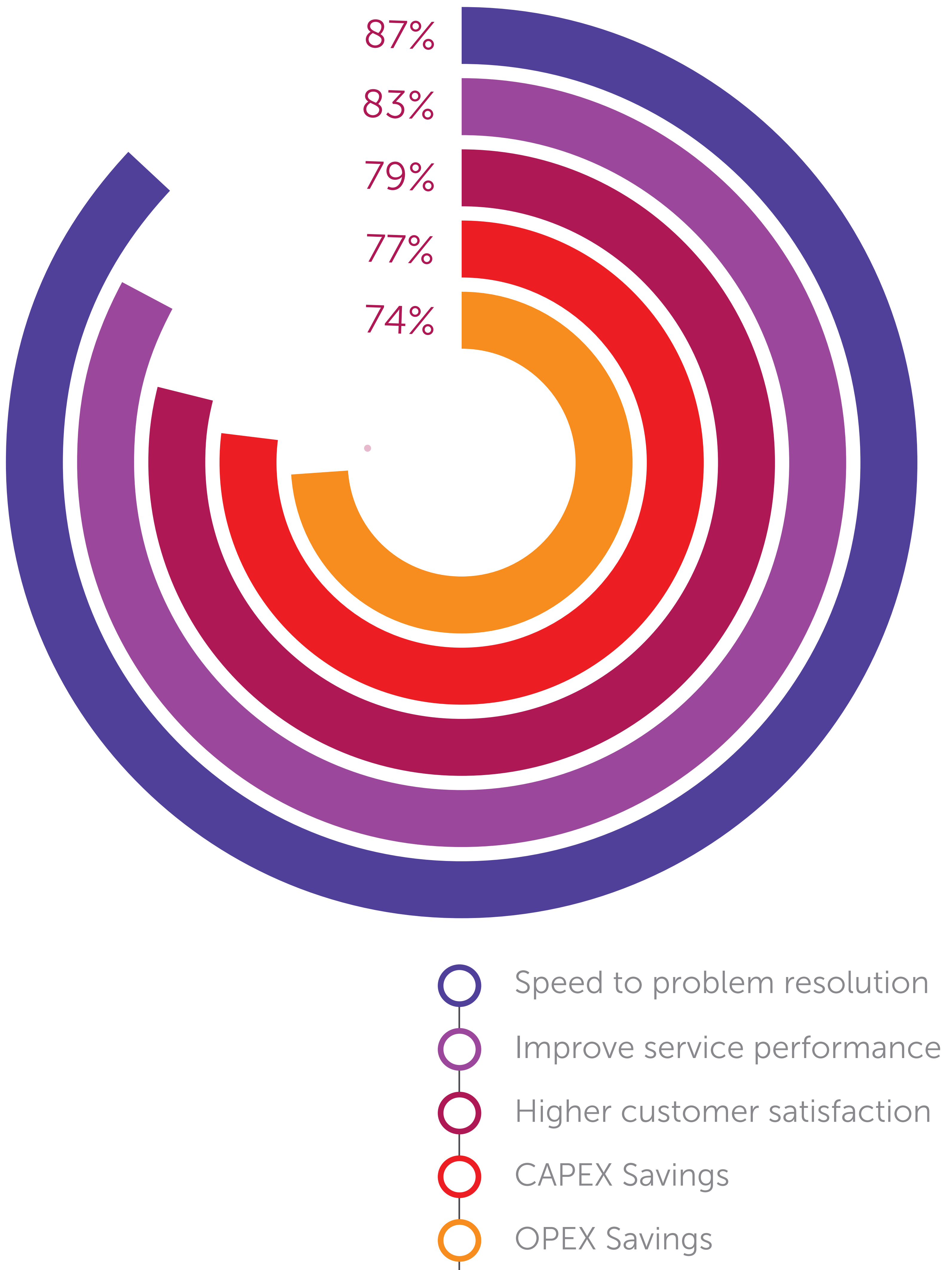
5 Areas Where CSPs Find Value in CLA Today

We asked CSPs where CLA is bringing them value today. Interestingly, they rated improving 'speed to problem resolution' and 'service performance' higher than achieving 'higher customer satisfaction', with CAPEX and OPEX savings not far behind.

In the US, CSPs were 30-50% likelier to rate customer satisfaction as the top reason.

Fewer Tier-3s rated higher customer satisfaction as a key benefit (62% vs 90% in tier 1 and tier 2 companies)

These findings conform with industry perceptions that the US is ahead of the customer-centric curve and that Tier 3s focus more on basic, low cost services.



KPIs or KQIs which will deliver improved QoE?

It's true that time to problem resolution and service performance will drive QoE improvement. But by looking at KPIs instead of KQIs, CSPs are still focusing on the "nuts and bolts" of the network.

By focusing on KPIs, CSPs show more concern about whether the pipe leaks rather than how good the water tastes! This doesn't bode well for CSP subscribers, who are motivated by the quality of their experience. In a the competitively priced mobile services market, QoE and ultimately customer satisfaction can translate into brand differentiation, high NPS and customer loyalty.

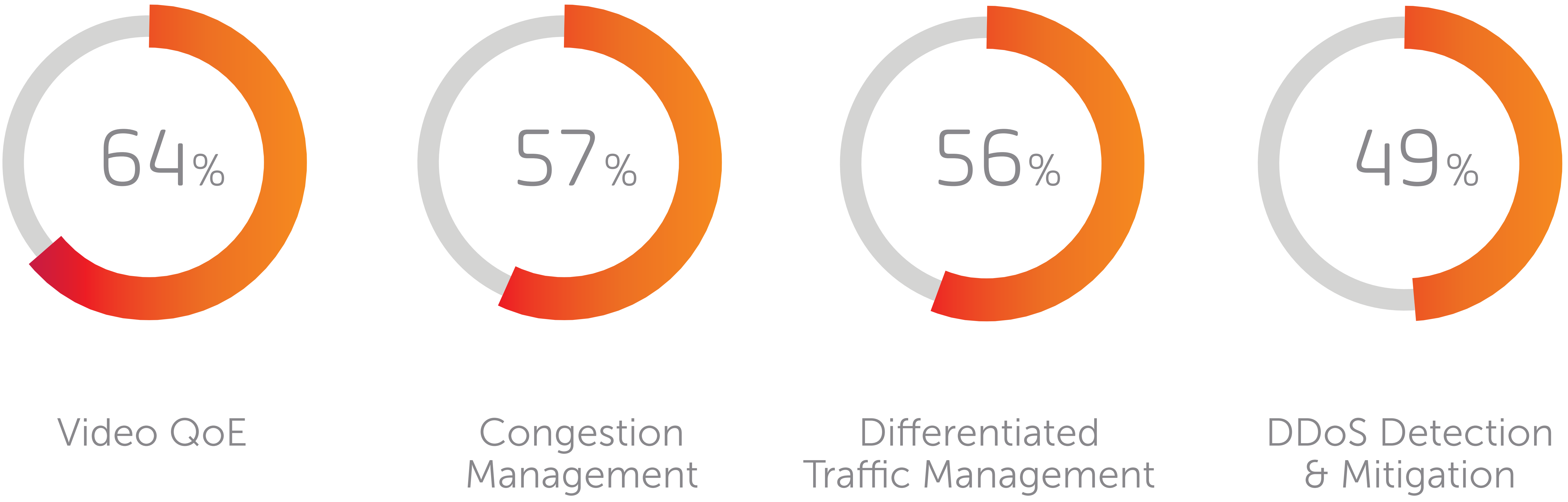
> *A 'mind shift' is still needed for CSPs to fully embrace customer-centric networking.*

CLA as a Network Management Tool

In the field, we found that most of today's solutions for Video QoE, congestion management, traffic management and DDoS mitigation typically revolve around KPIs. This may help with maintaining QoE, as it can affect network performance metrics. But, to truly impact customer experience, CSPs need to embark upon a customer-centric journey.

Where do CSPs deploy CLA as a network management tool today?

*The high percentages reflect that respondents were able to choose more than one use case.



> By looking at KPIs instead of KQIs, CSPs are still focusing on the “nuts and bolts” of the network.

Let's examine the differences between KPIs and KQIs by taking a close look at video QoE. A movie streamed on 4G networks may meet a certain KPI. But the customer’s perception will vary depending on whether they are watching from a TV or a small mobile device. If your KPI is aimed towards mobile customers, your TV viewer will not be satisfied. If you aim for TV viewers, both types of customers will be happy, but you will be over-provisioning and wasting valuable network resources.

KPIs vs. KQIs

SERVICE	NETWORK KPIs	EXPERIENCE KQIs
VIDEO STREAMING	BANDWIDTH, PACKET DROPS, RETRANSMITS	STALLS, RESOLUTION CHANGES, DEVICE-DEPENDENT RESOLUTION
CRITICAL COMMUNICATIONS	RETRANSMITS, PACKET DROPS	ON-TIME MESSAGE COMPLETION, MESSAGE LOSS
BROWSING	RETRANSMITS, PACKET DROPS	OBJECT LOAD TIME
GAMING	RETRANSMITS, PACKET DROPS	LAG, MESSAGE LOSS

It's All About Bandwidth Recovery

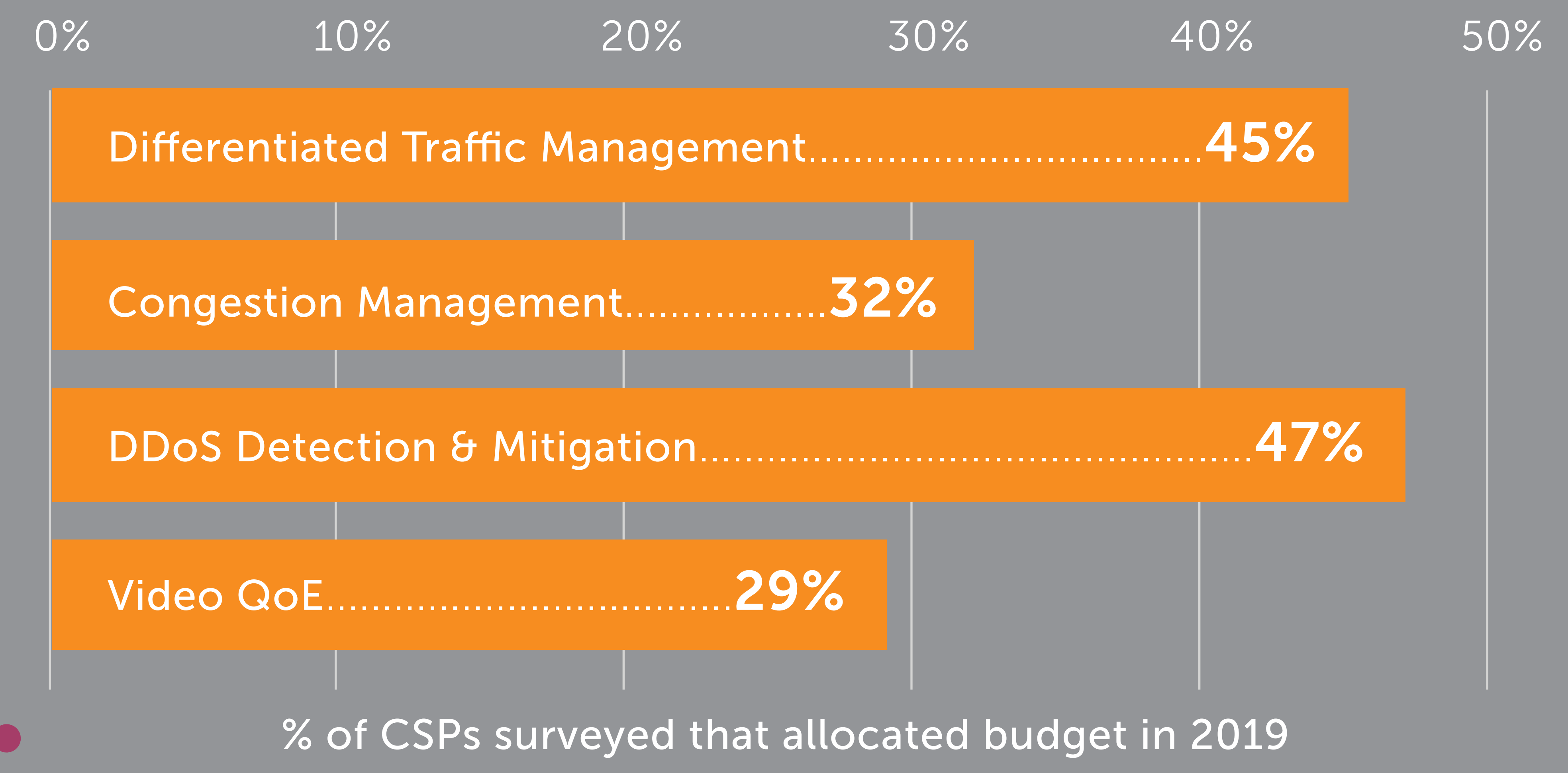
Recovering wasted bandwidth in 4G/LTE networks may well be the current CLA killer app.

Our survey results indicate that DDoS Detection/ Mitigation and Congestion Management are the top two use cases that CSPs would like to address using CLA.

28% DDoS Detection & Mitigation

26% Congestion Management

In addition, those CSPs that currently practice DDoS mitigation, rate congestion management as the CLA use case they want to implement next. And vice-versa.



The survey also showed that DDoS Detection/Mitigation is the most widely budgeted use case for 2019 (47% of CSPs). Clearly, CSPs see bandwidth recovery as a leading driver of CLA. The need is understood, and the ROI is straightforward. CSPs realize that money is being wasted by sub-optimal utilization of deployed infrastructure. In fact, our own experience with CSPs indicates that 10% of bandwidth capacity is being eaten by a combination of under-the-radar DDoS and inefficient congestion management.

What will be the CLA killer app for 5G?

In the Future

Home Yesterday Today In The Future Moving Forward

IoT Security: The Next Killer App for CLA

The arrival of 5G promises support for both Massive Machine Communication (MMC), and Critical Machine Communication (CMC) services, as well as extreme mobile broadband. Hence the industry anticipates an explosion of scale in IoT-based devices and services. CLA will have an important part to play.

Despite the industry hype, other studies show that security concerns are, in fact, the leading factor preventing widespread IoT deployment. Enterprises and CSPs are rightfully worried by the exponentially larger attack surface that widespread IoT presents. The media fuels those fears with frightening stories about compromised IoT devices wreaking havoc on networks around the world.

This would explain why more than two-thirds of our respondents strongly agreed that CLA has an important role in the growth of both Security and IoT Services, ahead of both CAPEX and OPEX savings.

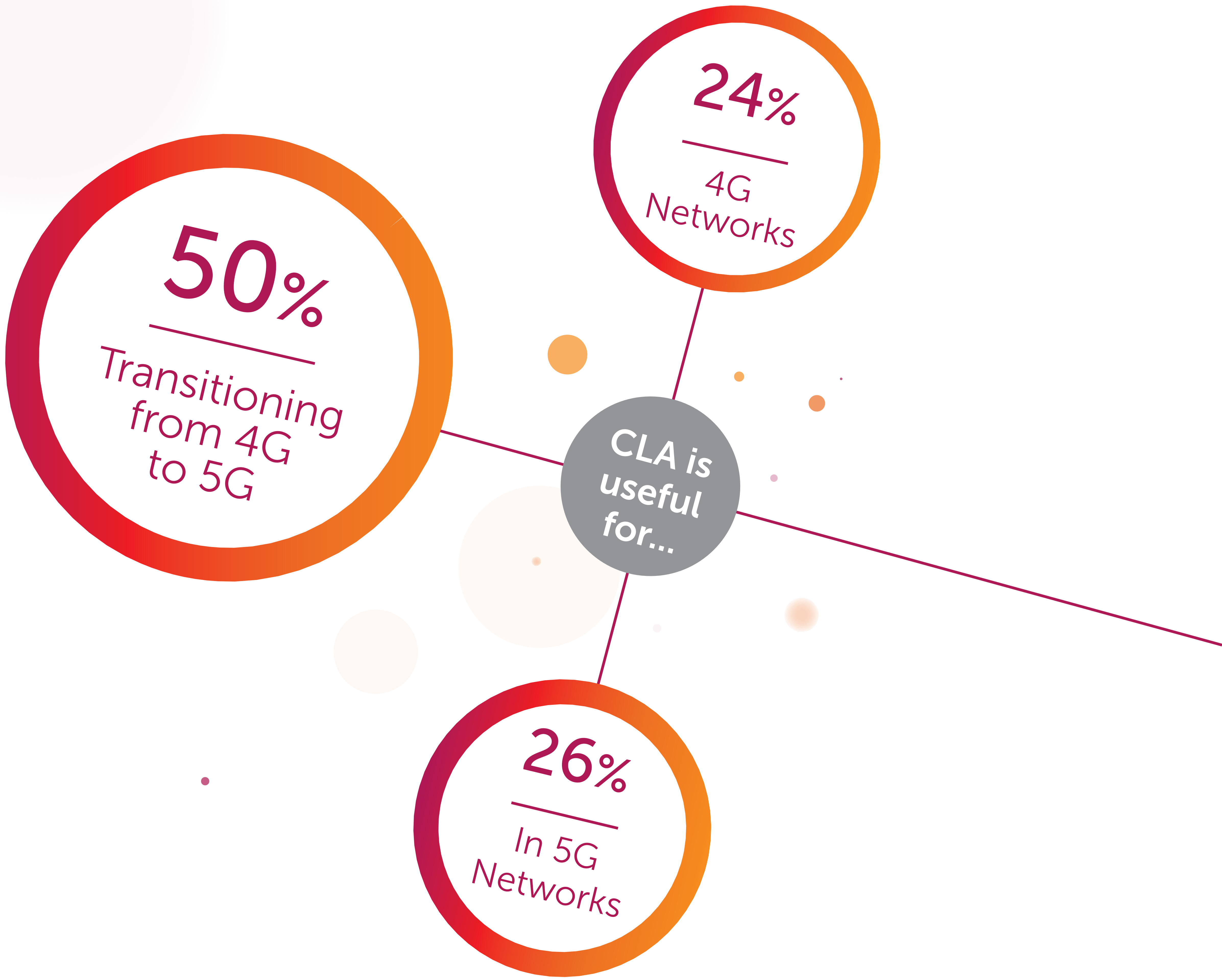
CSPs are clearly aware of the high vulnerability associated with IoT. Combined with the issues of scale, this makes a strong case that CLA should be a leading force for effectively mitigating IoT based threats today, and more importantly, as we move to 5G.

CLA:
The Bridge between Today and Tomorrow

It's clear that CSPs are busy planning for a future with 5G. During the transition, they must get the most out of their 4G infrastructure in order to cope with the constant increase in network traffic. Automation can maximize profitability during the transition.

So where, along the journey towards 5G, does CLA fit?

To find out, we asked where CLA provides the greatest value. Do CSPs see CLA adding the most value in 4G networks, during transition from 4G to 5G, or perhaps only once they have fully migrated to 5G?



> CSPs want to leverage existing 4G infrastructure while reallocating resources during the transition to 5G.

Despite the benefits that CLA provides in 4G networks, three-quarters of respondents feel that CLA will be most important in either the transition period (50%) or once they have fully implemented 5G (25%).

This is consistent with the commonly held view that during every technological transition, automation helps maximize profitability. CSPs clearly understand that they need to get the most out of existing 4G infrastructure while reallocating resources during the transition to 5G.

These findings may also indicate that CSPs understand the need to prepare for 5G's inherent CLA capabilities, by gaining experience during the transition. That way, they can more easily apply it when they reach 5G.

CLA in Tomorrow's 5G Networks

Much of the 5G hype is around its intelligent, service-based networking capabilities. Perhaps that is why a quarter of our surveyed CSPs indicated that CLA will be "most important during 5G". But do they see 5G's inherent CLA functionality as a cure-all capability or do they expect more?

3 Challenges as Networks Become Customer Centric

- ✓ Bandwidth always becomes constrained by rising demand
- ✓ Network optimization does not necessarily equate with an improved customer experience
- ✓ Cybercriminals will find new and creative ways to exploit 5G

Will a service-based network without additional CLA functionality be enough?

Consider this: Focusing on average end-to-end KPIs could, for example, cause a CSP to miss out on fine-tuning the individual session QoE of a premium package gamer. A service-based network that optimizes network Key Performance Indicators (KPIs) still does not guarantee higher Key Quality Indicators (KQIs) and a corresponding improved Quality of Experience (QoE).

And then there's security. 5G's massive bandwidth and IoT deployments will bring a dramatically larger threat landscape.

This will necessitate third-party, CLA-driven mitigation solutions to protect carrier networks and ensure application specific QoE for defined service segments.

All of the above are compelling reasons to implement advanced CLA functionality, now and as the industry moves towards 5G.

But some things are easier said than done.

A 5G CLA Scenario

With CLA, a fire marshal's emergency app would get priority service in order to receive instantaneous updates from a burning office building's smoke and fire detectors – even with a massive DDoS attack in progress.

Moving Forward

Barriers to Deployment

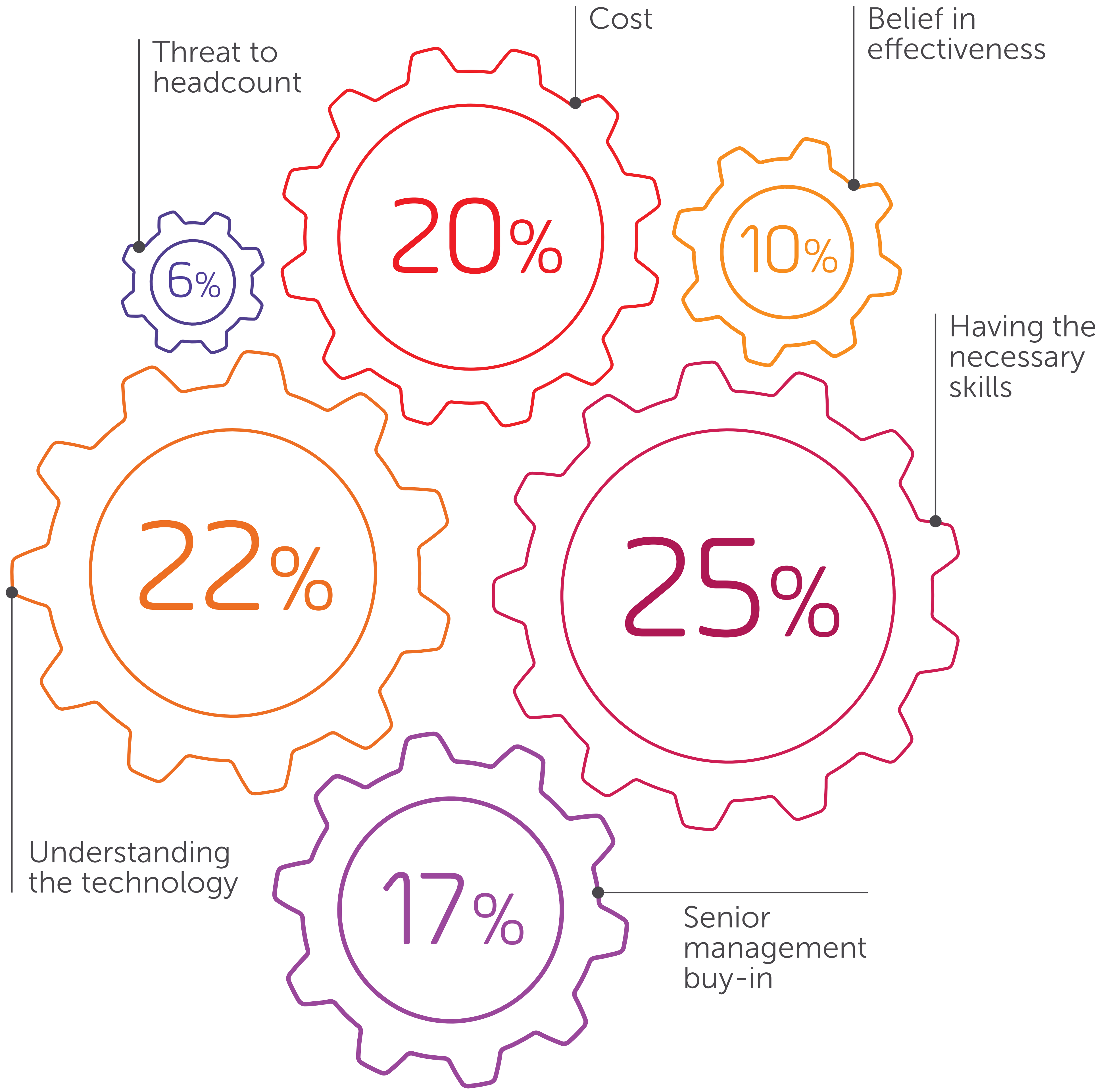
The advantages of CLA are quite evident, and it's clearly not just a 'nice to have'. In fact, according to a recent Light Reading article, "network operators need to be moving faster, or find themselves left behind". In a nutshell, they need to "automate or die".

Why do CSPs need to automate?
Complementing our survey's findings, the article points to 5G and IoT as the main drivers that will compel CSPs to embrace CLA. Our survey shows that it's clear CSPs understand the need for CLA even today.

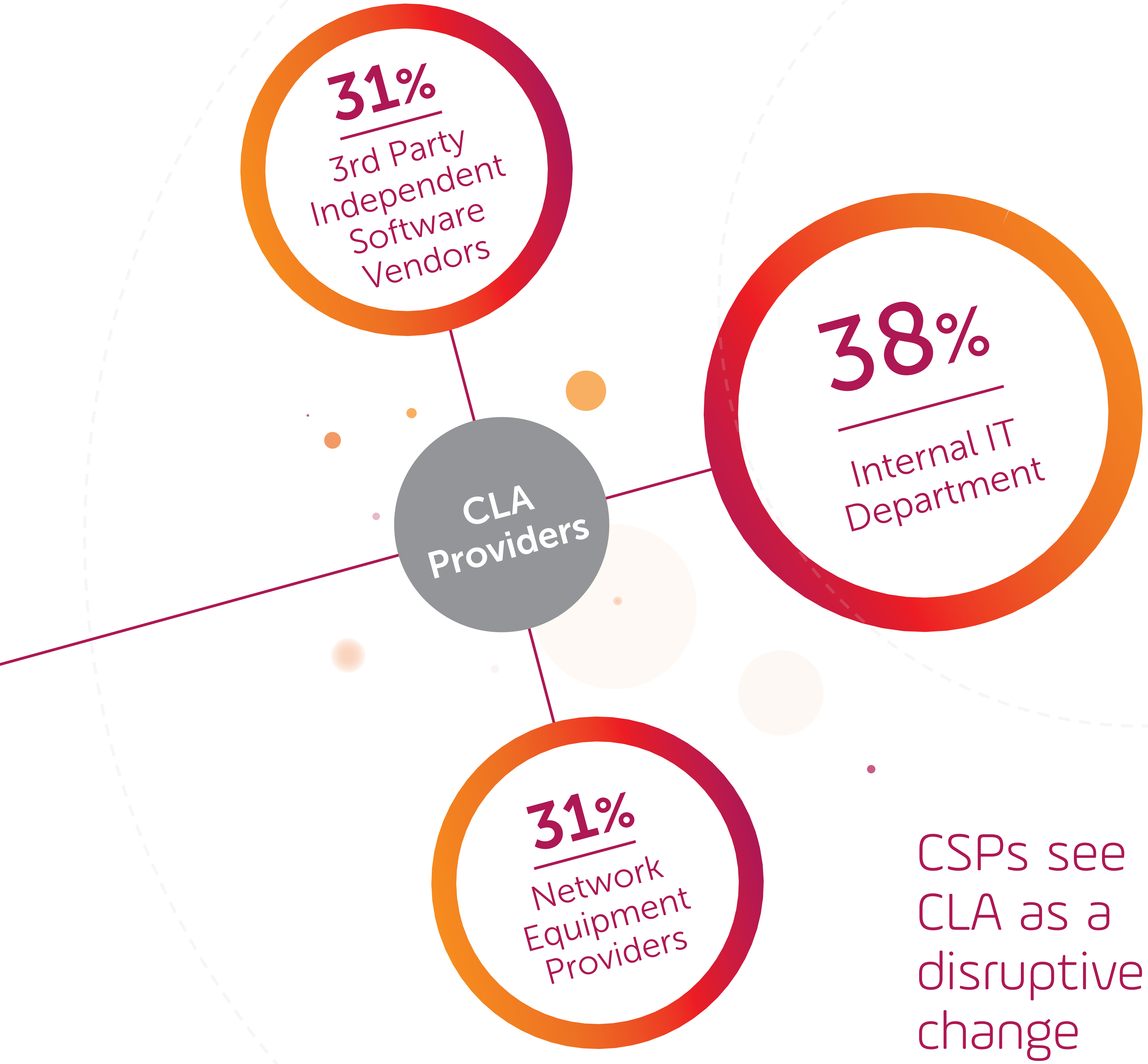
But it does beg the question: If CSPs consider CLA highly beneficial, even imperative, why aren't they deploying it more widely?

To find out, we asked them to rate their strongest obstacles to implementing CLA.

For almost half of those surveyed, it's about a lack of skillset or understanding of the technology.



Barriers to implementing CLA solutions



CSPs see CLA as a disruptive change

> It takes more than a NEP to address today’s growing threats.
>
> CSP Security Specialist

CSPs want the benefits of CLA. But they don’t want to grapple with the disruptive changes that introducing new skillsets and workflows would no doubt entail. That would explain why almost two-thirds of CSP respondents prefer to get their CLA tools and guidance from a third-party, rather than seeking an in-house solution.

Among that two-thirds, we discovered another interesting fact when analyzing respondents by department. Almost half of security personnel preferred using an independent software vendor (ISV) rather than relying on their network equipment providers (NEP). They understand that meeting security challenges requires solutions from security specialists.

The Secret Sauce:

Artificial Intelligence, powered by Machine Learning to solve challenges

ISVs can leverage technologies like Machine Learning (ML) and Artificial Intelligence (AI), to create software that learns to identify unknown problems and solve them automatically, based on anomalous behavior, learned patterns and applied models and policies that adjust on the fly when confronted with new data.

An instructive example of this approach would be the ability to identify zero-day DDoS attacks by benchmarking normal traffic and building up a knowledge base of learned variants of normal behavior. New, unknown attack patterns and traffic anomalies could then be identified and mitigated based on learned intelligence concerning normal and abnormal traffic. Furthermore, in a world of weaponized IoT, ML could detect unknown, anomalous device behavior and AI could implement throttling or quarantine policies to limit potential damage.

Another example relates to video traffic encryption. Identifying and evaluating video traffic quality has become extremely challenging. With YouTube, Netflix, and others encrypting their traffic, CSPs can no longer take the network-based approach of measuring KPIs for these applications. Traditional monitoring tools cannot identify the encrypted traffic and cannot decipher embedded, encrypted measurements.

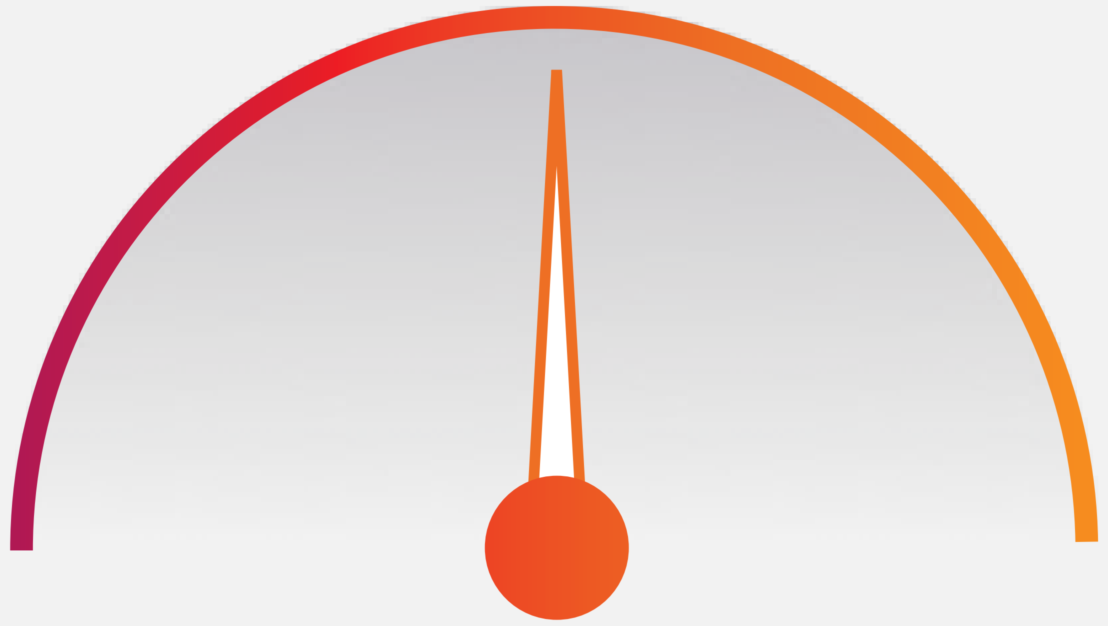
What is needed are innovative ISV solutions that leverage ML to detect encrypted video and utilize AI to infer KQIs and deduce from them the end users' experience. CLA will then take this customer-centric approach one step further by automatically tweaking relevant network parameters to ensure sustained, optimal QoE.

3 Results from CLA Powered by AI and Machine Learning

Reduce Big Data Fatigue

Leverage AI based analytics to extract easily understood actionable intelligence from enormous amounts of raw data

Defy Encryption



Use ML to uncover which applications and services are consuming bandwidth or not meeting expectations

Detect and Isolate Dynamic Threats

Marshal ML and AI to spot and stop new anomalies before they stop your network

Your Customer-Centric, CLA-Enhanced Journey

We have pinpointed a number of issues affecting CSPs today that can be mitigated by CLA.
Take a look at the list of network operational issues and the CLA-powered solutions which can help you improve your QoE.

Operational Challenges		CLA-Powered Solutions
The Cost of Capacity Expansion	»	Congestion management & DDoS mitigation
Balancing Backhaul Consumption and QoE	»	Traffic shaping and QoE assurance
Encrypted Video Quality of Experience	»	ML-driven video classification and optimization
QoE of Business Critical Applications	»	Application detection and prioritization
Top Tier Customer Satisfaction	»	Service plan based, equitable prioritization
Content Specific SLA and QoE Assurance	»	Content detection and prioritization
The Next BIG DDoS Attack	»	Anomalous traffic detection & mitigation
Weaponized IoT Running Wild	»	Host Based Anomaly Detection & quarantining
Enterprise Customer SLAs	»	Throughput policy enforcement
Reallocating resources for migration to 5G	»	Everything!

Home Yesterday Today In The Future Moving Forward

CLA Key Takeaways

Embracing CLA is a Must

CSPs realize they need to embrace CLA and that failure to deploy it widely will prove costly.

CLA is a Journey

As CSPs in all tiers continue the journey towards becoming more customer centric, they will better appreciate the need for CLA and realize its advantages.

IoT and Security will Drive CLA Adoption

IoT growth and security needs will be the main drivers for CLA adoption.

But for CSPs to take full advantage, they need CLA that focuses on end-user QoE, not just network KPIs.

Think Growth, Think ISV

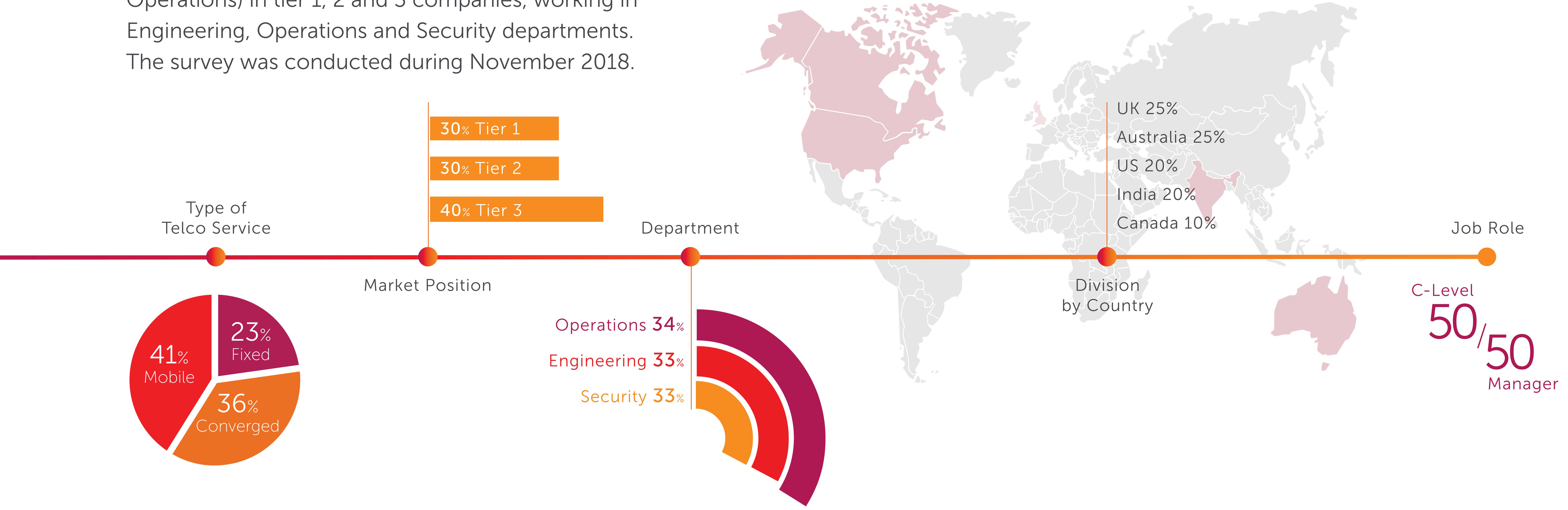
Independent Software Vendors (ISVs) are best positioned to deliver CLA with the ML and AI capabilities that cost-effectively ensure optimal performance, security and Quality of Experience.

The CLA Inherent in 5G is Not Enough

5G Networks, by design, will feature CLA that handles known problems. But to address and solve unforeseen problems, and to meet QoE expectations, will require additional CLA functionality, powered by AI and ML.

Survey Methodology

The audience was made up of 100 senior management/ C-suite respondents (e.g. CTO, Head of Engineering/ Operations) in tier 1, 2 and 3 companies, working in Engineering, Operations and Security departments. The survey was conducted during November 2018.



Type of Telco Service

41% Mobile

23% Fixed

36% Converged

Market Position

30% Tier 1

30% Tier 2

40% Tier 3

Department

Operations 34%

Engineering 33%

Security 33%

Division by Country

UK 25%

Australia 25%

US 20%

India 20%

Canada 10%

Job Role

C-Level 50/50 Manager

Home
Yesterday
Today
In The Future
Moving Forward

Resources

- Frost & Sullivan: Closed Look Automation – A strategic Imperative for Today's CSPs
- Frost & Sullivan: Optimze QoE with Automated Intelligence
- Allot: Congestion Management: QoE Assurance through Automated QoE & DDoS Mitigation
- neXt Curve: Contextually-Aware Mobile Security as a Service
- neXt Curve: The Democratization of 5G Everything
- neXt Curve: Crossing the 5G and IoT Connectivity Chasm
- Light Reading: It's Simple - Automate or Die
- Networkworld: A Primer on Closed Loop Automation
- Inform: Closed-Loop Implementation
- TelecomTV – The Automation Journey Towards 5G Networks

Allot is a leading provider of innovative network intelligence and security solutions that empower communications service providers (CSPs) and enterprises worldwide to enhance the value they bring to their customers. With over 20 years of proven success, our solutions turn network, application, usage and security data into actionable intelligence that make our customers' networks smarter and their users more secure.

Allot's multi-service platforms are deployed globally, in the most demanding environments, by over 500 mobile, fixed and cloud service providers and over a thousand enterprises. We support evolving network architectures by offering the most flexible platforms in the market, including COTS hardware, software only and field-proven, fully NFV compliant solutions.

allot

sales@allot.com | www.allot.com