5G Network & Service Strategies Operator Survey

Produced by

LightReading

HEAVY READING

In Partnership with

atis

5G americas

Sponsored by

BAE SYSTEMS

EMPIRIX

intel

JUNIPER NETWORKS

Radisys

Red Hat

VIAVI

Introduction

This Heavy Reading 2021 **5G Network & Service Strategies Operator Survey** is designed to provide insight into how 5G networks and services will evolve as operators and the wider mobile ecosystem invest in and develop 5G technology. This is the third annual version of the survey, and it comes after almost a full year of disruption caused by the COVID-19 pandemic.

Developed in association with the report sponsors, the online questionnaire was fielded to respondents in the Light Reading service provider database in January and February 2021. It was open only to employees of communications service providers (CSPs).

This report analyzes the results of the survey in the following thematic sections:

- 5G service strategies: Scaling for the mass market
- 5G radio access network (RAN) evolution
- 5G core networks
- 5G edge cloud
- 5G transport networks
- 5G and lawful intercept
- 5G enterprise services
- 5G testing and service assurance
- 5G edge and endpoints

The questionnaire received a total of 82 responses from individuals who self-identified as working for CSPs. Rogue, suspicious, and non-operator responses were removed. Technical, engineering, and network operations personnel from large operators in advanced markets account for the majority of the responses. The US is the dominant region, with as many responses as the rest of the world combined; however, all major global regions were represented. **Figures 1 – 4** show the survey demographics. **Figure 5** shows that 50% of respondents work for operators that already offer 5G service; this reflects the rapid rollout of 5G globally over the past two years.

Figure 1:
What type of telecom service provider do you work for?

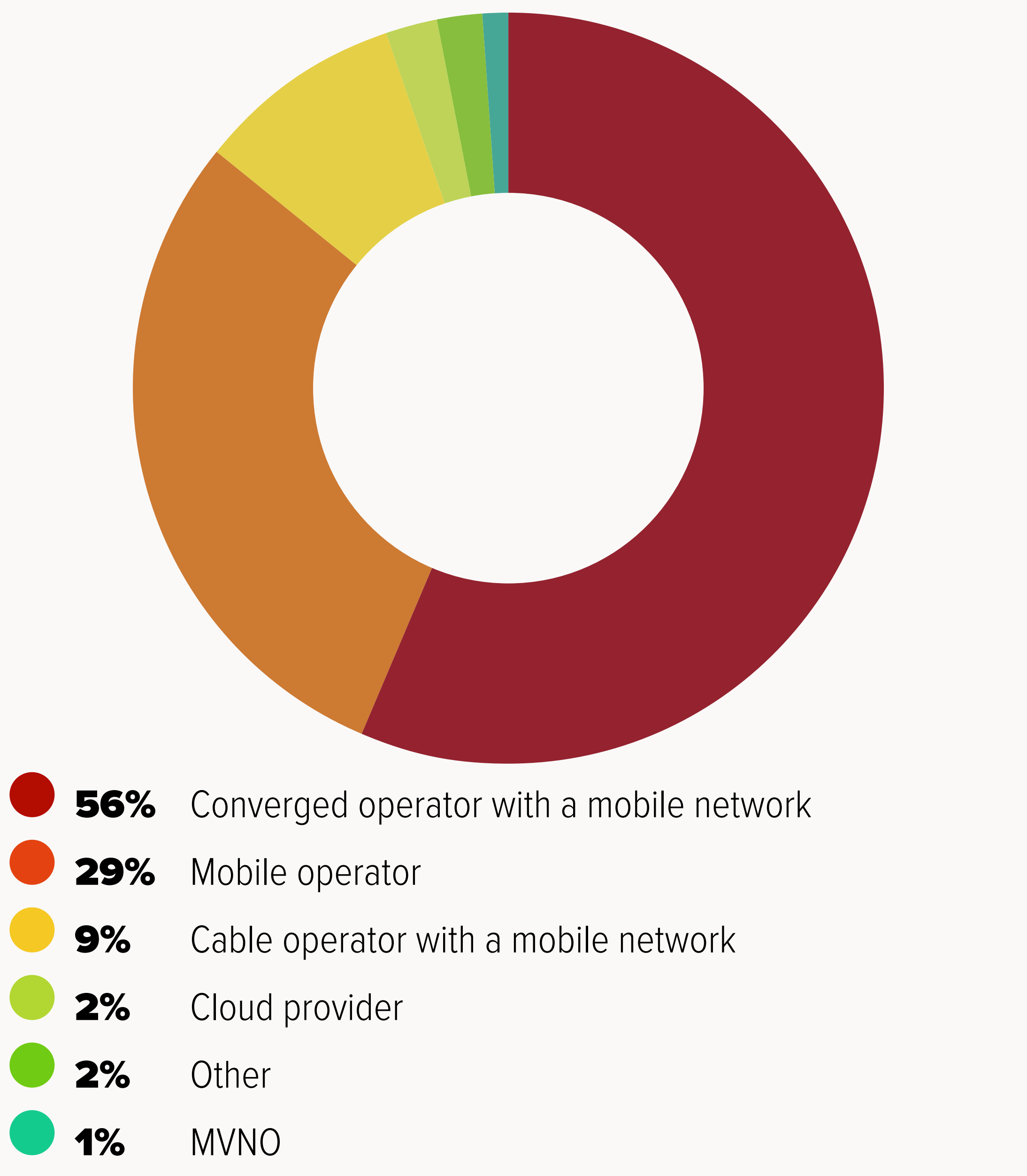


Figure 2:
In what region is your organization headquartered?

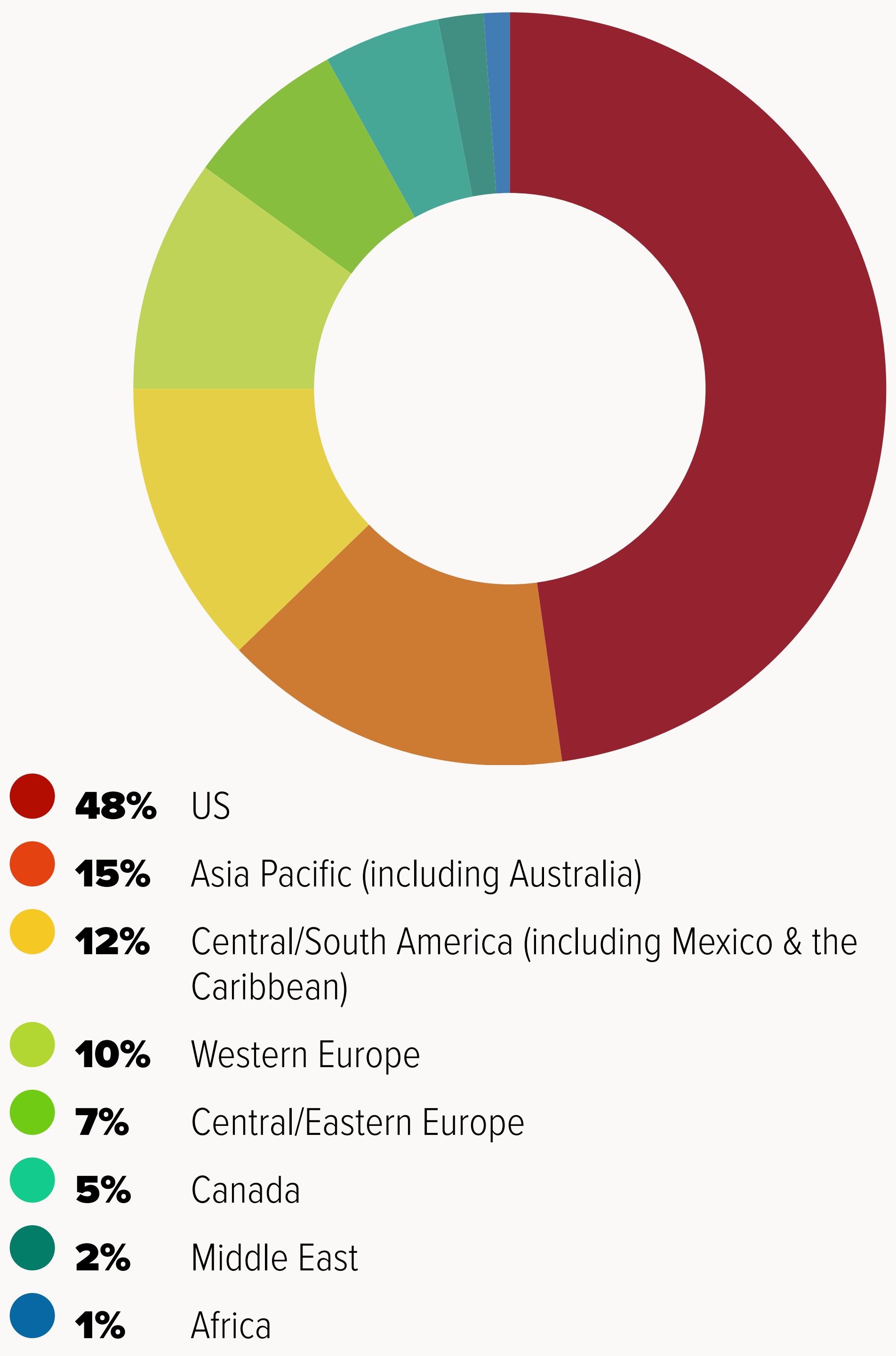


Figure 3:
What is your primary job function?

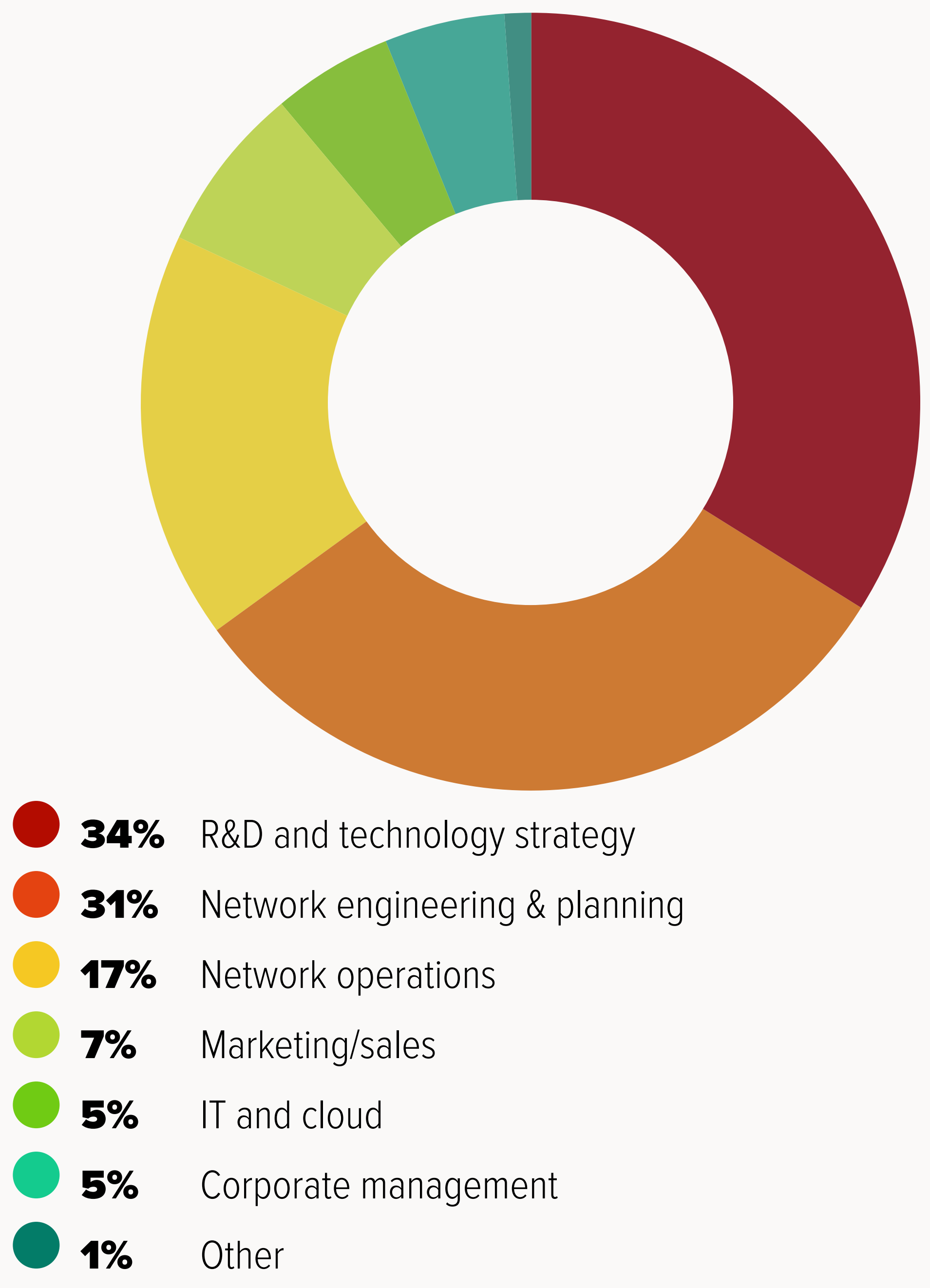


Figure 4:
What is your organization's approximate annual revenue?

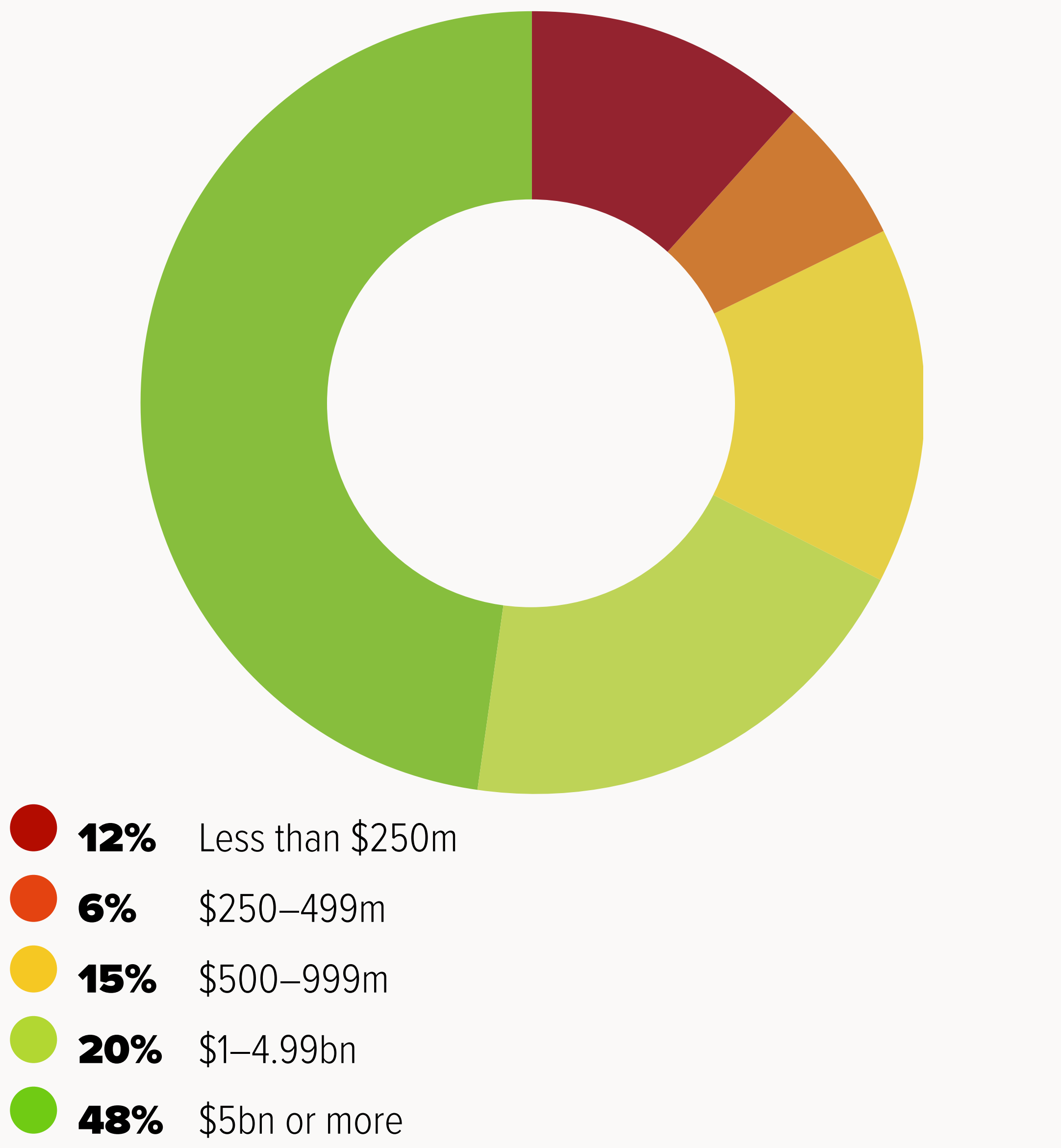
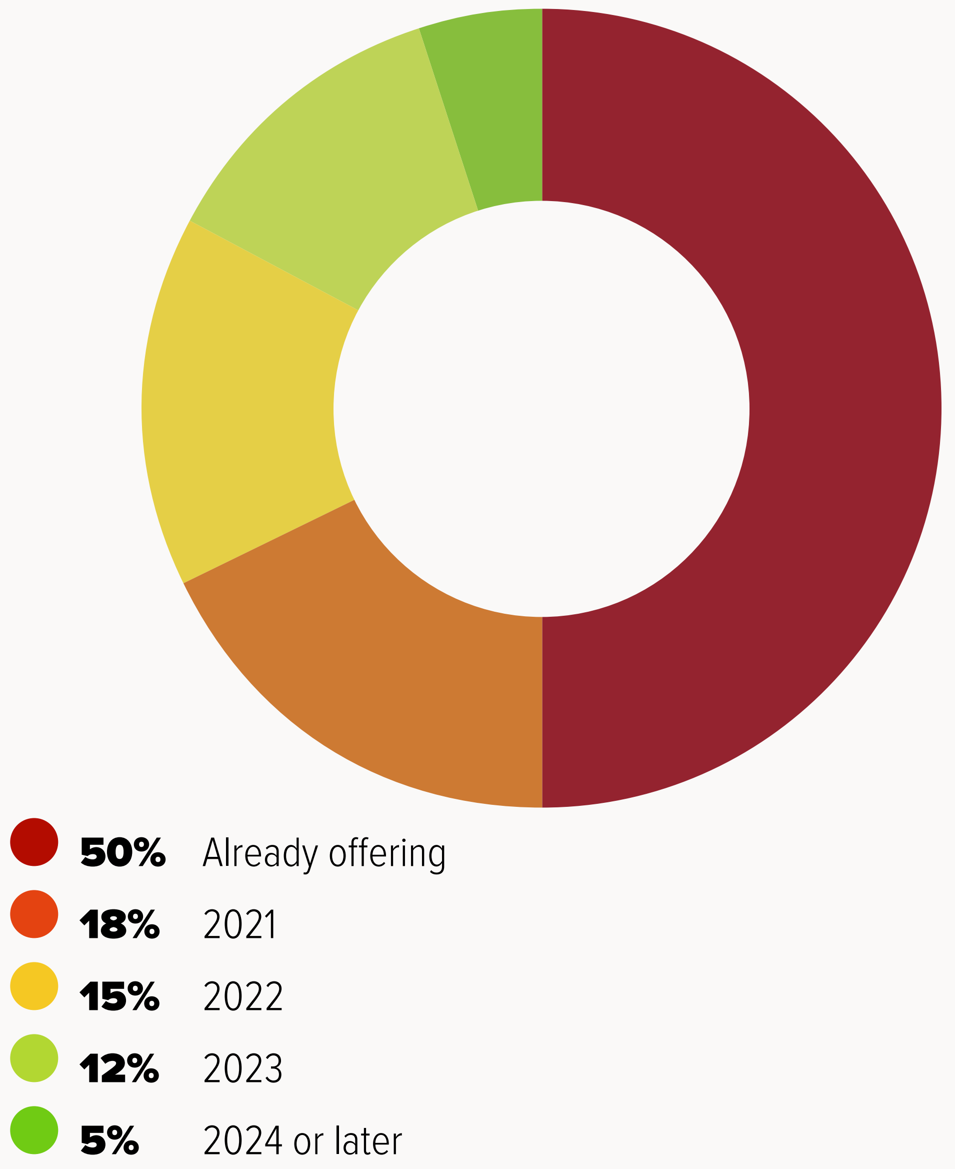


Figure 5:
When does your organization expect to launch 5G services commercially?



Report Authors

Gabriel Brown: Senior Principal Analyst – Mobile Networks & 5G

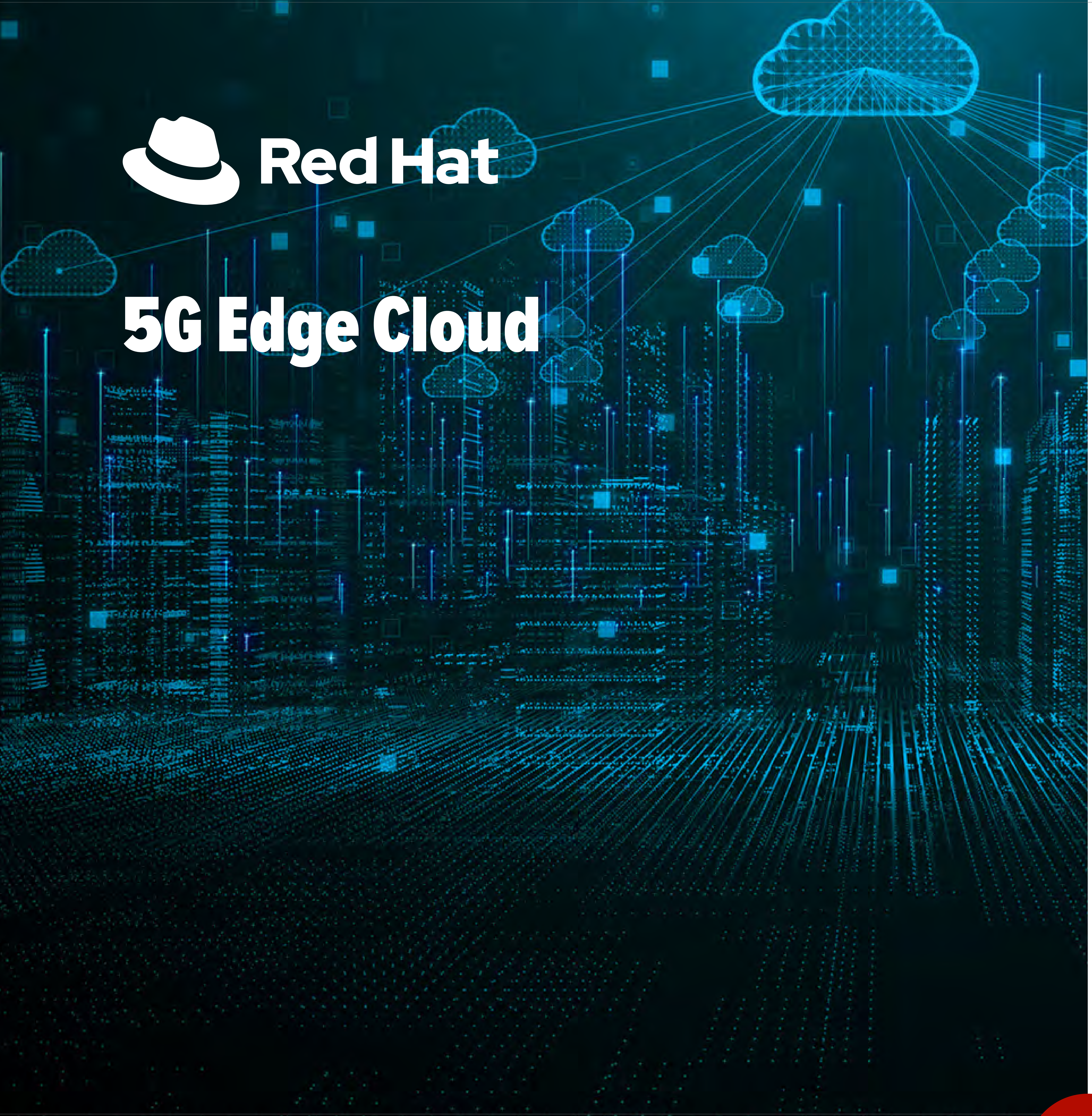
Gabriel leads mobile network research for Heavy Reading. Starting from a system architecture perspective, his coverage area includes RAN, core, and service-layer platforms. Key research topics include 5G, LTE Advanced, virtual RAN, software-based mobile core, and the application of cloud technologies to mobile networking. Gabriel has more than 15 years' experience as a mobile network analyst. Prior to joining Heavy Reading, he was Chief Analyst for Light Reading's Insider research service; before that, he was editor of IP Wireline and Wireless Week at London's Euromoney Institutional Investor.

Jim Hodges: Research Director – Cloud & Security

Jim leads Heavy Reading's research on the service assurance and security impact of the virtualized cloud on the control plane and application layers, both in the fixed and mobile core and at the enterprise edge. Jim focuses on the security impacts that cloud-based technologies such as 5G introduce from a cyber-threat detection perspective, as well as billing and service assurance transformation implications. Jim joined Heavy Reading from Nortel Networks, where he tracked the VoIP and application server market landscape and was a key contributor to the development of Wireless Intelligent Network (WIN) standards. Additional technical experience was gained with Bell Canada, where he performed IN and SS7 network planning, numbering administration, technical model forecast creation and definition of regulatory-based interconnection models. Jim is based in Ottawa, Canada.

Sterling Perrin: Senior Principal Analyst – Optical Networks & Transport

Sterling has more than 20 years' experience in telecommunications as an industry analyst and journalist. His coverage area at Heavy Reading is optical networking, including packet-optical transport and 5G transport. He also authors Heavy Reading's Metro Optical Networking Market Tracker and Core Optical Transport Market Tracker. Sterling joined Heavy Reading after five years at IDC, where he served as lead optical networks analyst, responsible for the firm's optical networking subscription research and custom consulting activities. Prior to IDC, Sterling worked for Standard & Poor's, where he delivered global industry analysis on a range of IT segments. He is a former journalist and editor at Telecommunications Magazine. In addition to chairing and moderating many Light Reading events, Sterling is a NGON & DCI World Advisory Board member and past member of OFC's N5 Market Watch Committee. Sterling is a highly sought-after source among the business and trade press.



5G Edge Cloud

By Gabriel Brown, Senior Principal Analyst, Mobile Networks & 5G, Heavy Reading

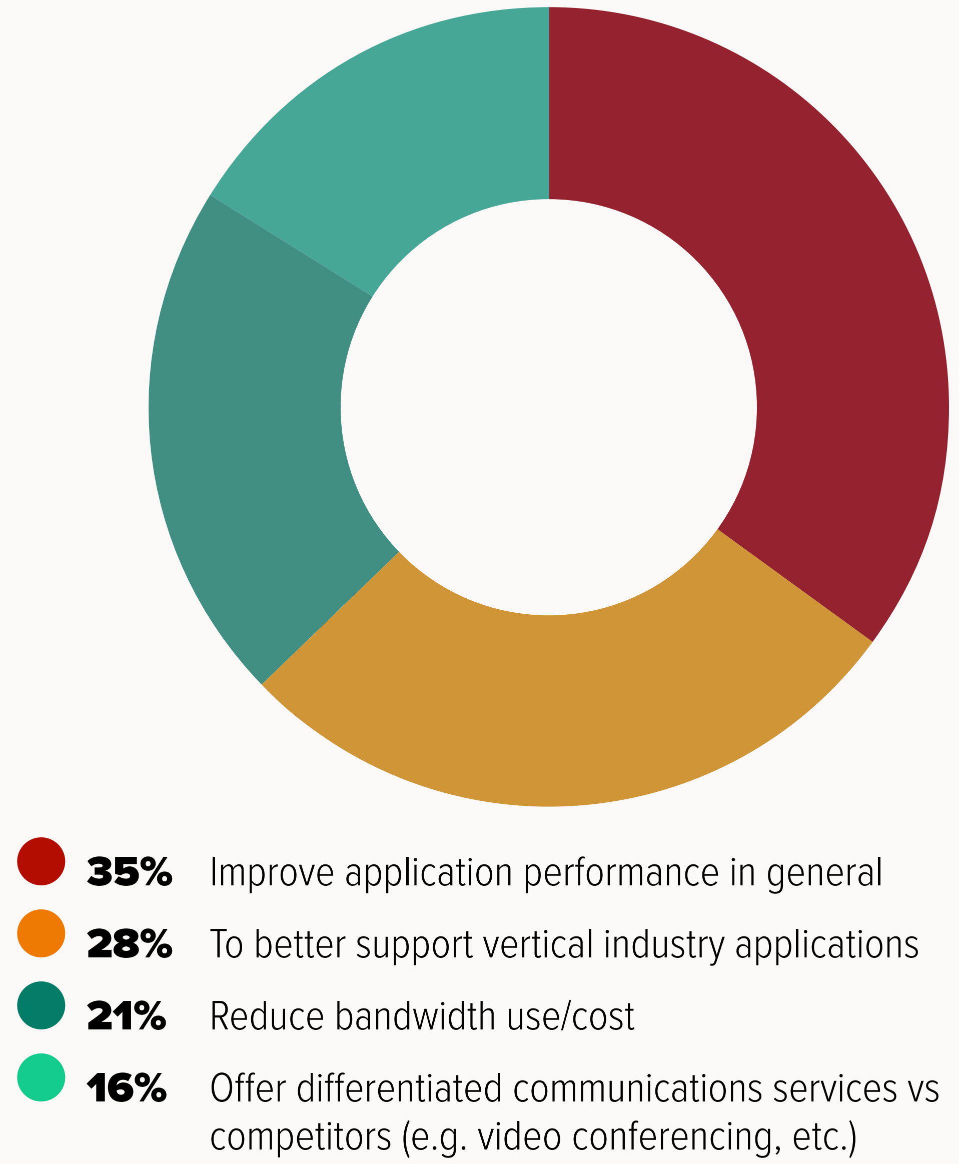
The 5G network architecture enables operators to deploy edge cloud infrastructure to radically improve how services perform on mobile networks. By hosting applications and content closer to customers, operators can make the best use of high bandwidth low latency access and deliver the advanced services for which 5G is designed. The deployment of edge infrastructure has many variables and is expected to occur in phases. This section of the survey investigates some of the key steps that operators must take as they implement this new service delivery architecture.

The key findings for this section are as follows:

- To “improve application performance in general” is the leading reason operator respondents give for investing in the 5G edge, which, with a score of 35%, is just ahead of “to better support vertical industry applications” with 28% and to support “differentiated communication services” with 16%, and to “reduce bandwidth use/cost” with 21%. These results indicate that operators will focus their 5G edge strategies on end-user services, rather than on efficiency.
- Operators are bullish on the timeline for the edge with 18% planning to offer services this year, a large 49% next year, and then 21% in 2023. This makes an 88% commitment to edge services over the next three years. The conclusion, therefore, is that activity related to edge architecture, vendor selection, and deployment, will be high in the near term.
- The two biggest perceived barriers (cost and complexity at 32% and availability of certified use cases at 26%) tell the story of 5G and the edge as it exists today: a good idea with great potential, but one that needs development and investment over a sustained period to become a mainstay of 5G service delivery.

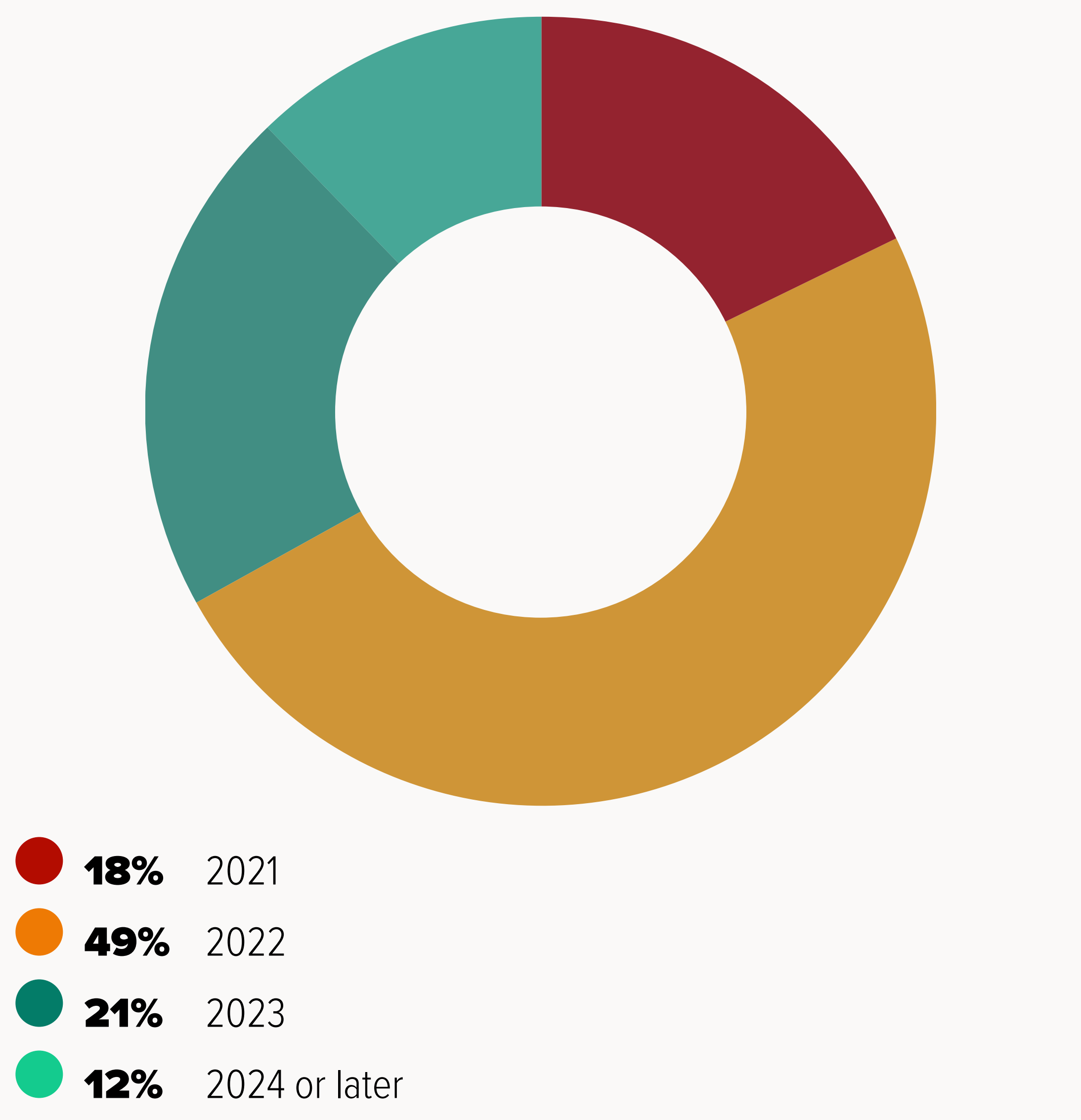
It is always useful to ask why a new technology or architecture is needed. **Figure 21** shows that operators have a wide variety of motivations to move workloads to the edge. The largest response, as might be expected, is to “improve application performance in general” with 35%. In second and third place are the 28% with the intention “to better support vertical industry applications” and the 16% that aim to “offer differentiated communication services,” both of which, in combination, show that many operators will be targeted in their edge performance strategies. On the efficiency side, “to reduce bandwidth use/cost” scores a solid 21%. The overall picture, therefore, shows a strong bias toward improving service performance, but with a split between an intention to improve services in general and those with an intention to be more targeted.

Figure 21:
What is your primary motivation to move workloads to the edge?



Operators are bullish on the timeline for the edge with 18% planning to offer services this year, a large 49% next year, and then 21% in 2023. This makes an 88% commitment to edge services over the next three years, according to **Figure 22**. This probably paints an overly optimistic picture of the schedule and it might be better to think that this result reflects the ambitions of the advanced operators that predominate in the survey demographic. Nevertheless, the data is clear: operators are committed to the edge and activity related to architecture, vendor selection, and deployment will be high in the near term.

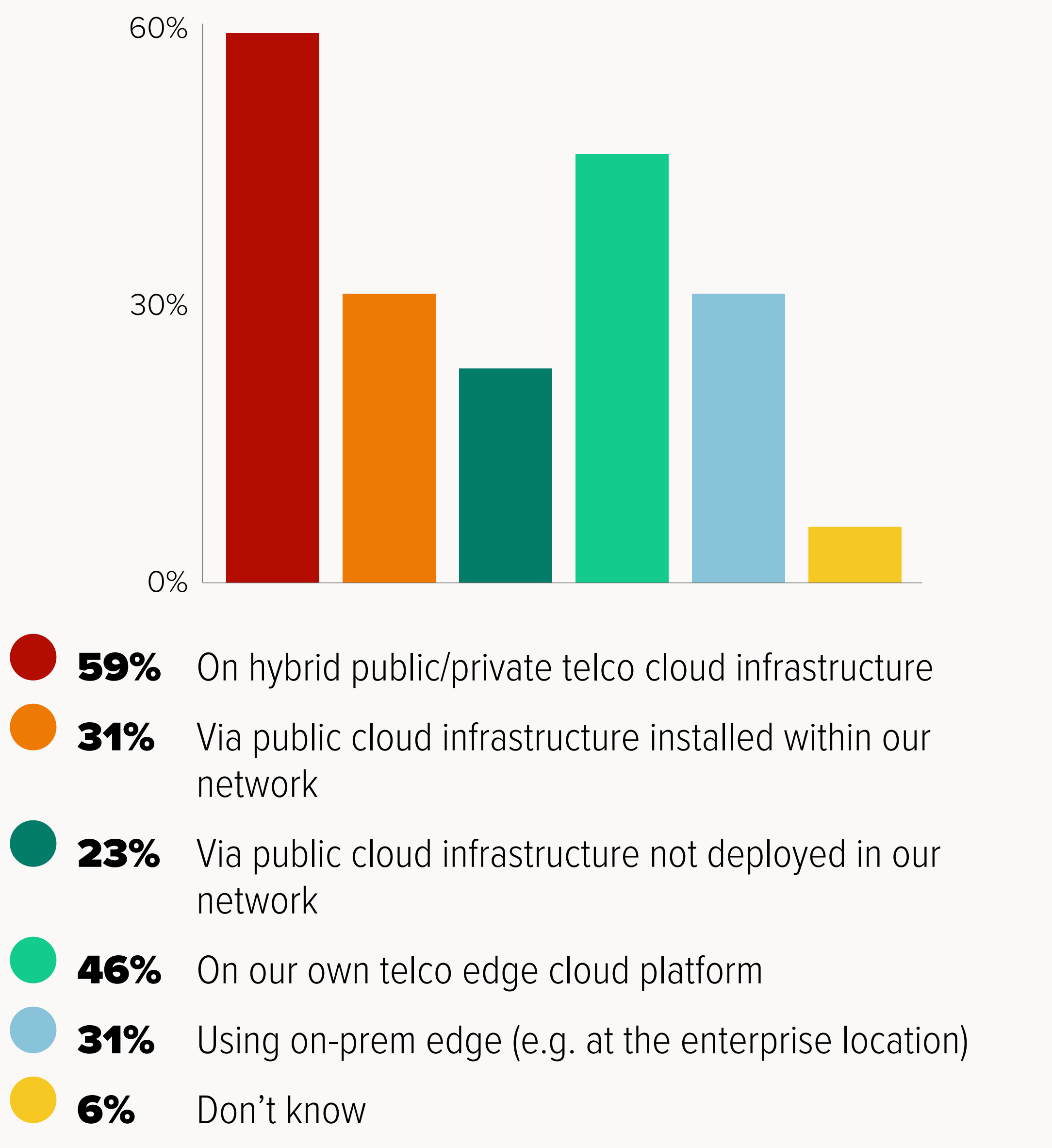
Figure 22:
When will your organization start to offer 5G edge services?



The next question asks how operators will offer edge services and, specifically, on what kind of infrastructure? This is a "select all that apply" question to reflect the likelihood that operators will pursue multiple edge strategies. There are 160 votes from 82 individual respondents, which indeed shows that operators will employ diverse strategies.

Nevertheless, **Figure 23** shows a clear preference, with a majority (59%) selecting "hybrid public/private telco cloud infrastructure" some distance ahead of the other options. In second, with 46%, is "on our own telco edge cloud platform." Both cases show, unsurprisingly, that operators favor edge cloud models that make use of their own unique network infrastructure. The advantages of owning and controlling network assets are also seen in the third-place option of "public cloud infrastructure installed within our network" at 31%, which comes ahead of "public cloud not deployed within our network" at 23%.

Figure 23:
How will your organization offer edge services?



The edge cloud is made up of diverse hardware (switches, servers, network interface cards [NICs], racks, power supplies, etc.), but this is generally considered software-defined infrastructure. Currently, there are two major solutions: virtualized infrastructure to run VNFs and cloud-native infrastructure to run CNFs. Cloud native is, as the name implies, more advanced, and is important at the edge for many reasons, particularly because when operating across a larger number of locations, automation is critical, and the need for centrally orchestrated solutions and efficient operation is, therefore, greater.

Figure 24 asks respondents to estimate the ratio of their company's workloads that are containerized today and will be by the end of 2023. This implicitly contrasts from virtualized workloads and is a way to get a feel for the rate at which the edge will move to cloud native. Only 17% (14% and 3%) say over half their workloads are already cloud native today. Over the next three years, this grows to 54% (36% and 18%). This increase is expected because cloud native is relatively new, but it is perhaps a little surprising that the transition to containerized workloads is not faster. The overall picture from the survey is that a combination of virtualized and containerized workload types will persist over the medium term.

Figure 24:
What percentage of your edge cloud workloads are containerized now and what percentage will be containerized by the end of 2023?

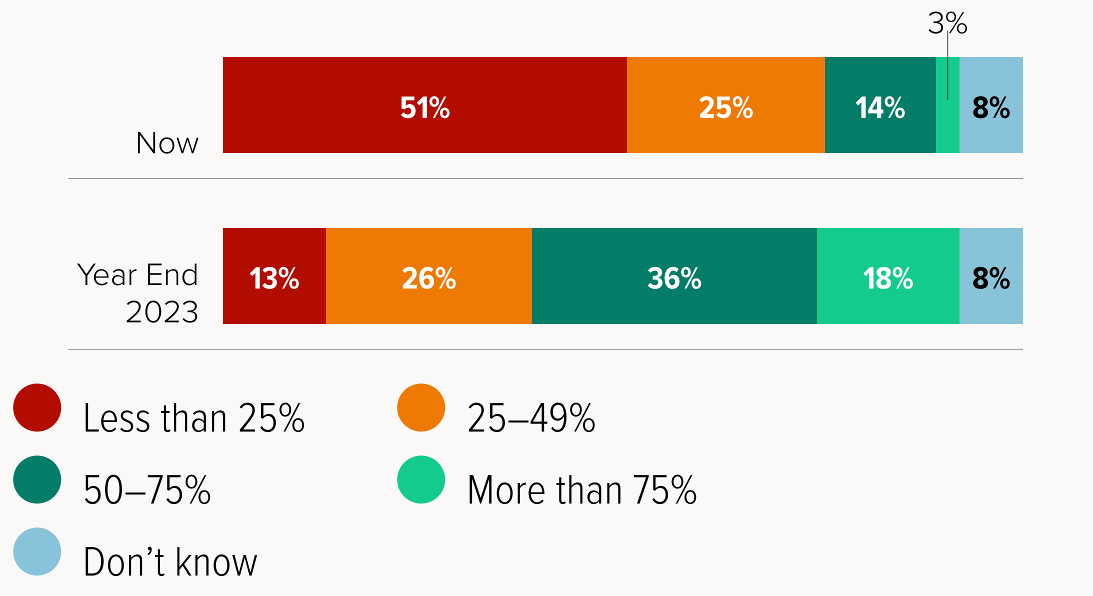
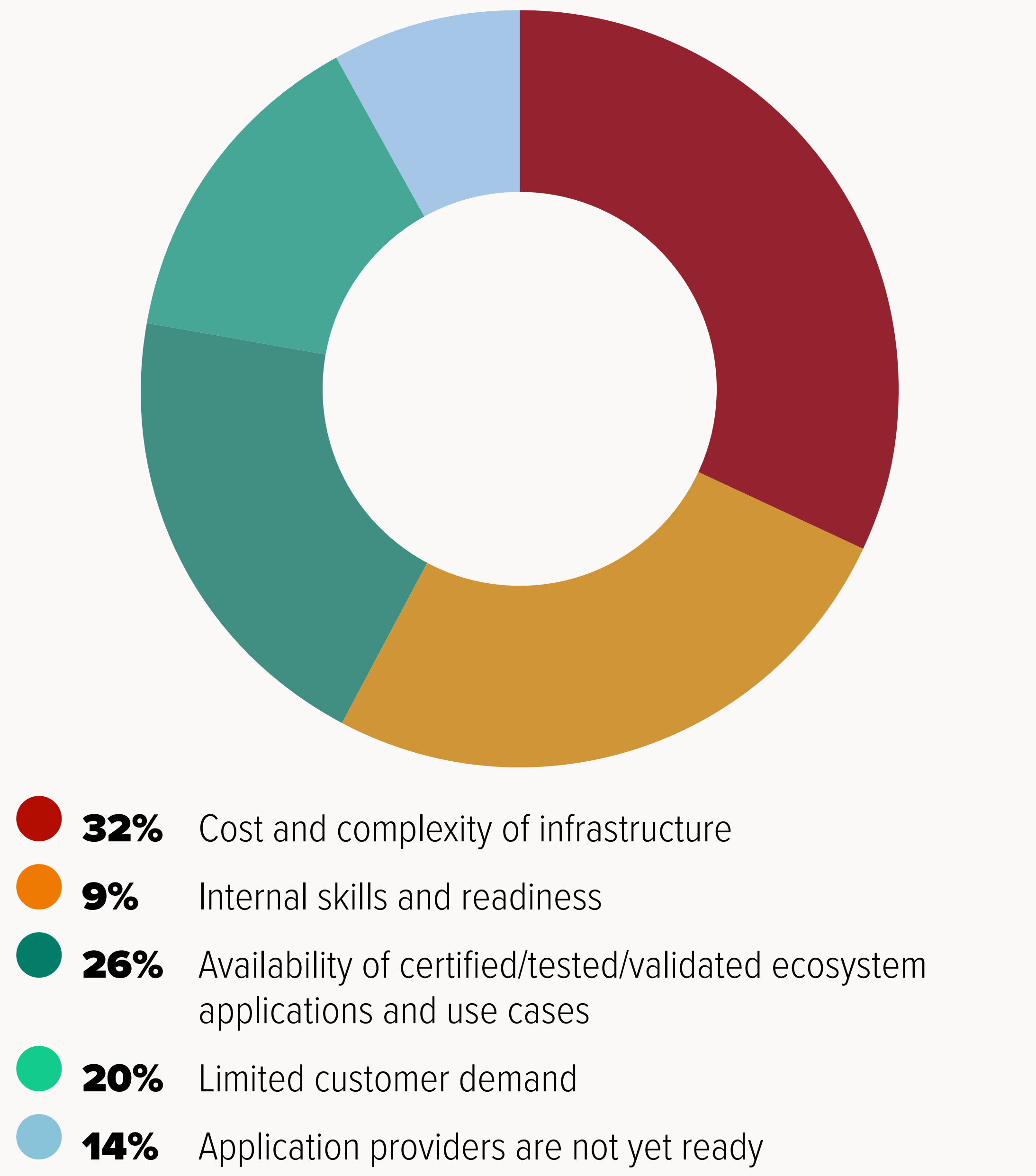


Figure 25 asks what is limiting 5G and edge cloud deployments. The response is evenly split. It is perhaps a surprise to see "internal skills" at only 9%, given that the edge is such a significant change in architecture and a new service delivery model. It is encouraging to see "limited customer demand" scores only 20%. The two biggest perceived barriers ("cost and complexity" at 32% and "availability of certified ... use cases" at 26%) tell the story of 5G and the edge as it exists today: a good idea with great potential, but one that needs development and investment over a sustained period to become a mainstay of the 5G service delivery.

Figure 25:
What is limiting your 5G and edge cloud deployment the most?



Red Hat

Executive Summary

Telecommunications providers who use the powerful combination of 5G with edge computing offer better user experiences and support bandwidth-hungry apps through a more flexible, agile, and resilient network. Using cloud-native solutions at the edge for their radio access networks (RANs) allows digital service providers to quickly scale software-based network functions. Using multi-access edge computing (MEC), service providers can enable large-scale, latency-sensitive applications for their enterprise customers.

As edge computing solutions mature, organizations are looking for a unified, horizontal platform—from the core to the edge—with a consistent deployment and operations experience. Red Hat provides the tools for agile integration, deployment and management of your applications at the edge to optimize as you scale the number of edge locations. Together with our ecosystem partners we help our customers make the most of edge computing without fear of fragmentation or lock-in. We know you have many different kinds of workloads in different locations (public cloud, private cloud). Our telco-grade edge solutions and hybrid cloud approach help you extend to the edge so that you can provide the experience your users expect, while also addressing cost, resilience and regulatory requirements.

Red Hat

Securing 5G Edge and Endpoints

Securing 5G Edge and Endpoints

By Jim Hodges, Research Director Cloud and Security, Heavy Reading

The delivery of low latency, high value 5G services at the edge introduces additional infrastructure and endpoint security requirements. This section documents the capabilities and strategies that operators plan to deploy at the edge to meet these new security demands.

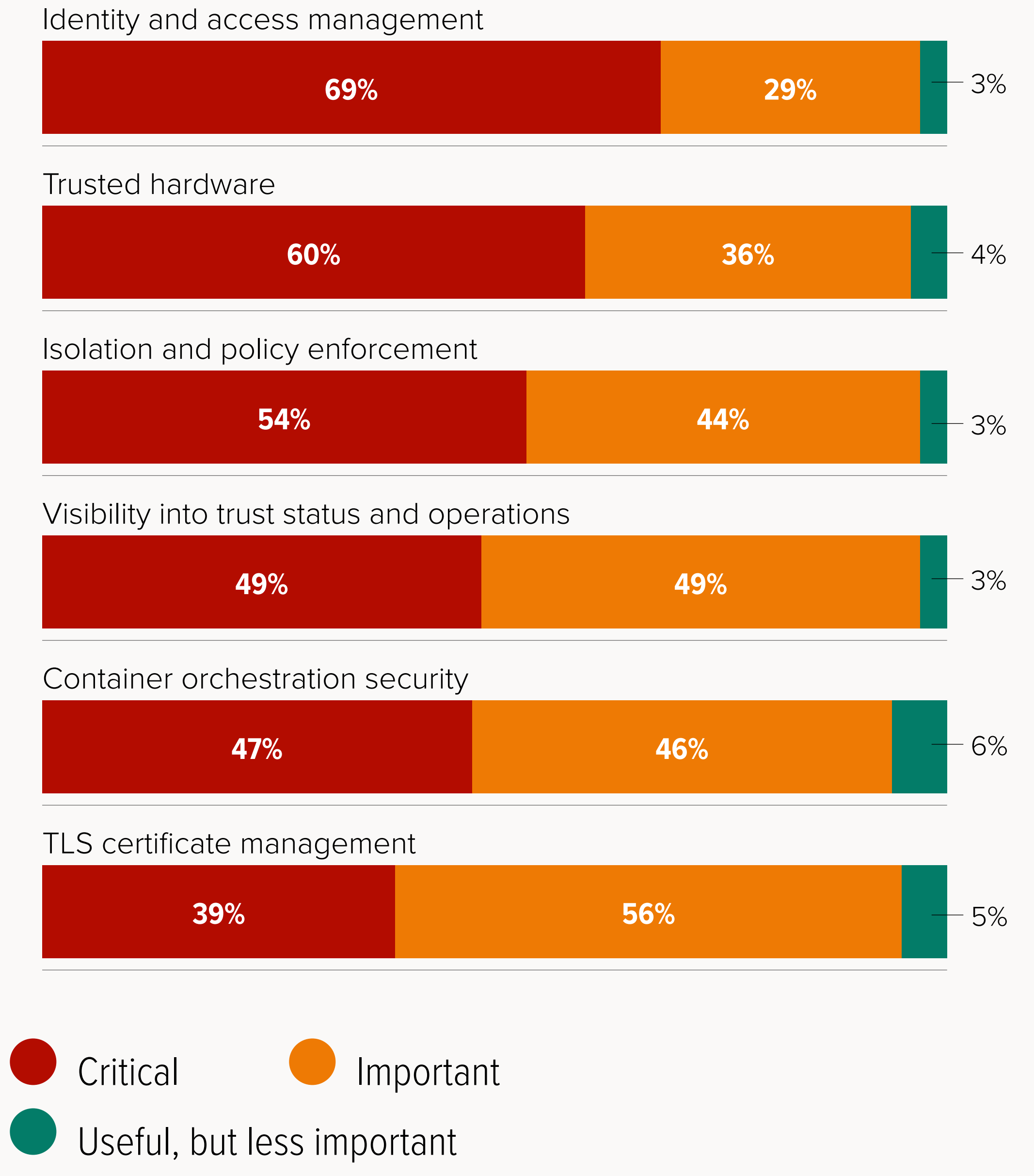
The key findings for this section are as follows:

- An effective 5G security strategy requires trust in both platforms and the software capabilities that run on them. Accordingly, trusted hardware ranked highly as a “critical” security capability for both 5G infrastructure in general (60%) and at the edge (68%).
- Operators plan to run advanced policy and trust-based security capabilities on these hardware platforms. “Critical” software priorities at the edge include establishing a strong root of trust for remote devices under management (63%) and enforcing a global security policy and posture (62%).
- Overall, operators are confident that their hardware and software strategies will enable them to secure edge infrastructure and end points. For example, 63–76% of operators believe they have in place a mature and scalable security strategy (63%) that is equipped with the resources and skillsets (76%) to support the new requirements associated with distributed infrastructure (72%).

In response to a fluid and dynamic threat landscape, operators pragmatically realize they must rely on a number of security capabilities to secure their 5G infrastructure. Of these, as shown in **Figure 45**, the leading “critical” capabilities are identity and access management (69%), trusted hardware (60%), and isolation and policy enforcement (54%). The input confirms that an effective 5G security strategy requires policy-based tools to support key functions, such as identity management hosted on trusted hardware platforms.

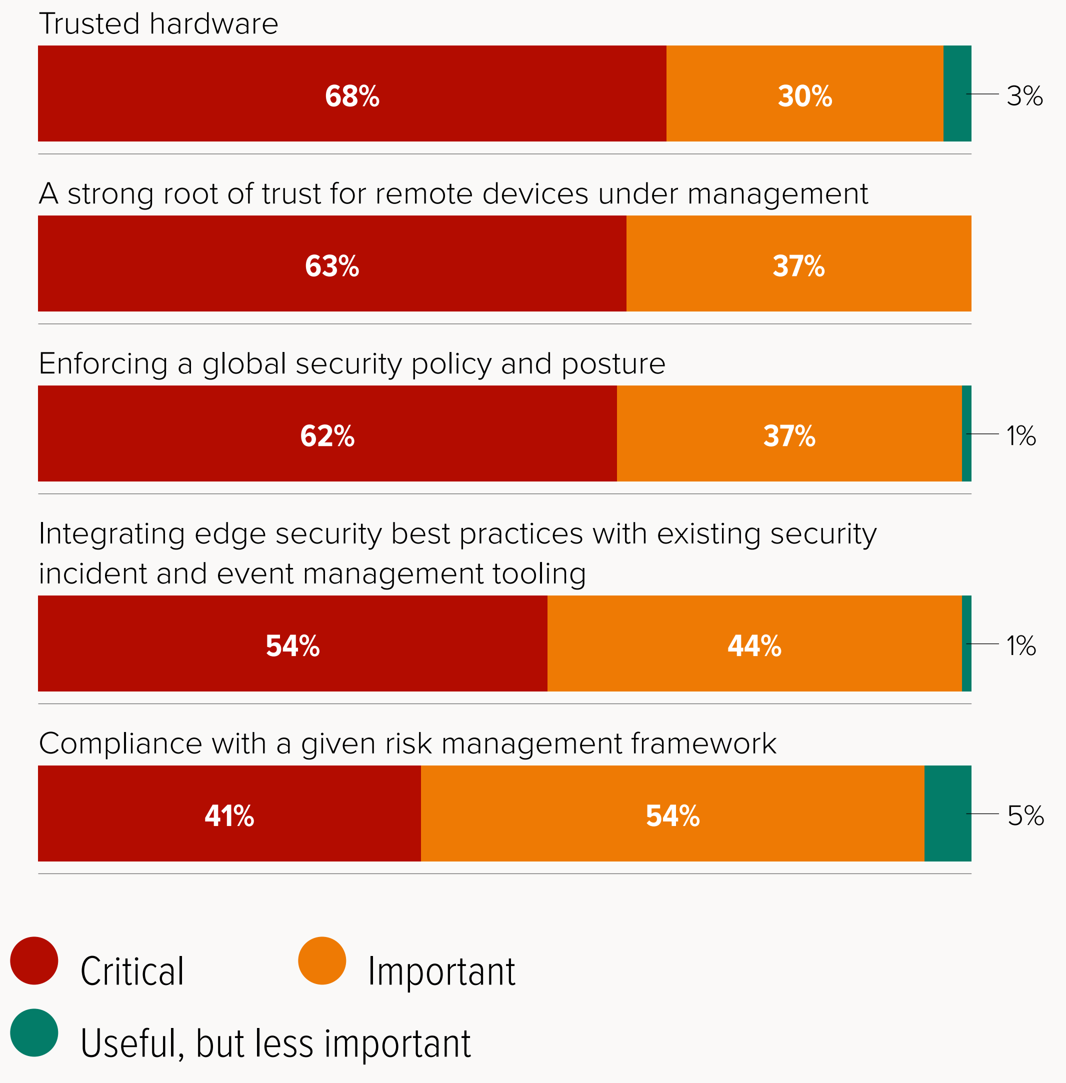
.

Figure 45:
How important are the following capabilities for securing 5G infrastructure at your organization?



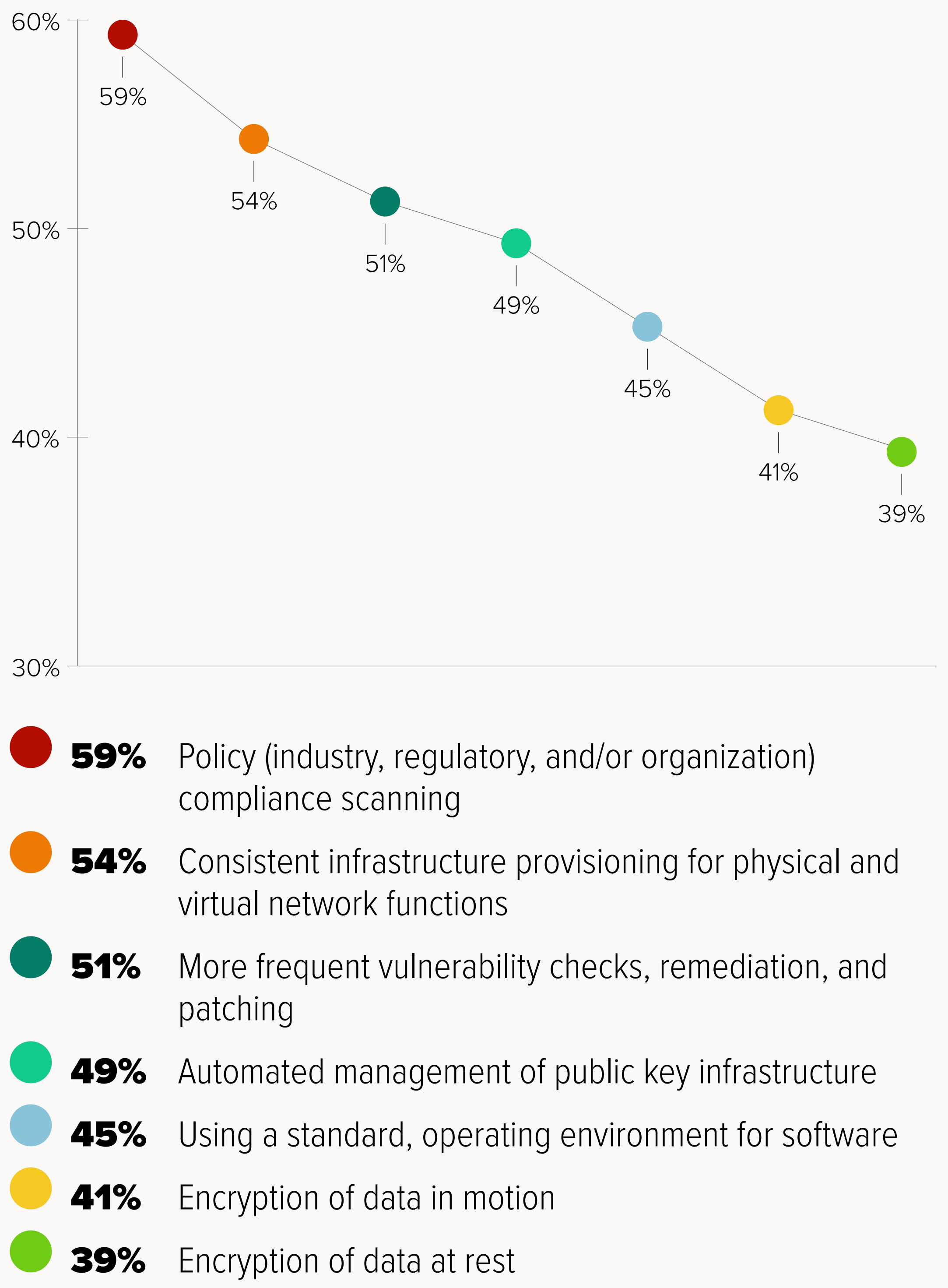
Trusted hardware is also a top consideration at the edge. As shown in **Figure 46**, it is, in fact, the leading “critical” capability (68%). In addition, software capabilities, such as management of remote devices, also attained a high “critical” ranking (63%), followed closely by enforcement of a global security policy and posture (62%).

Figure 46:
How important are the following capabilities for securing edge infrastructure at your organization?



As the 5G cloud evolves, so must 5G security strategies. To meet these needs, as **Figure 47** shows, operators are focusing on several capabilities. Of these, the top three leading capabilities are policy-based compliance scanning (59%), consistent infrastructure provisioning of physical and virtual network functions (54%), and more frequent vulnerability checks, remediation, and patching (51%). The fourth-place ranking of automated management of public key infrastructure (49%) reinforces that automation will be a vital element of future security models.

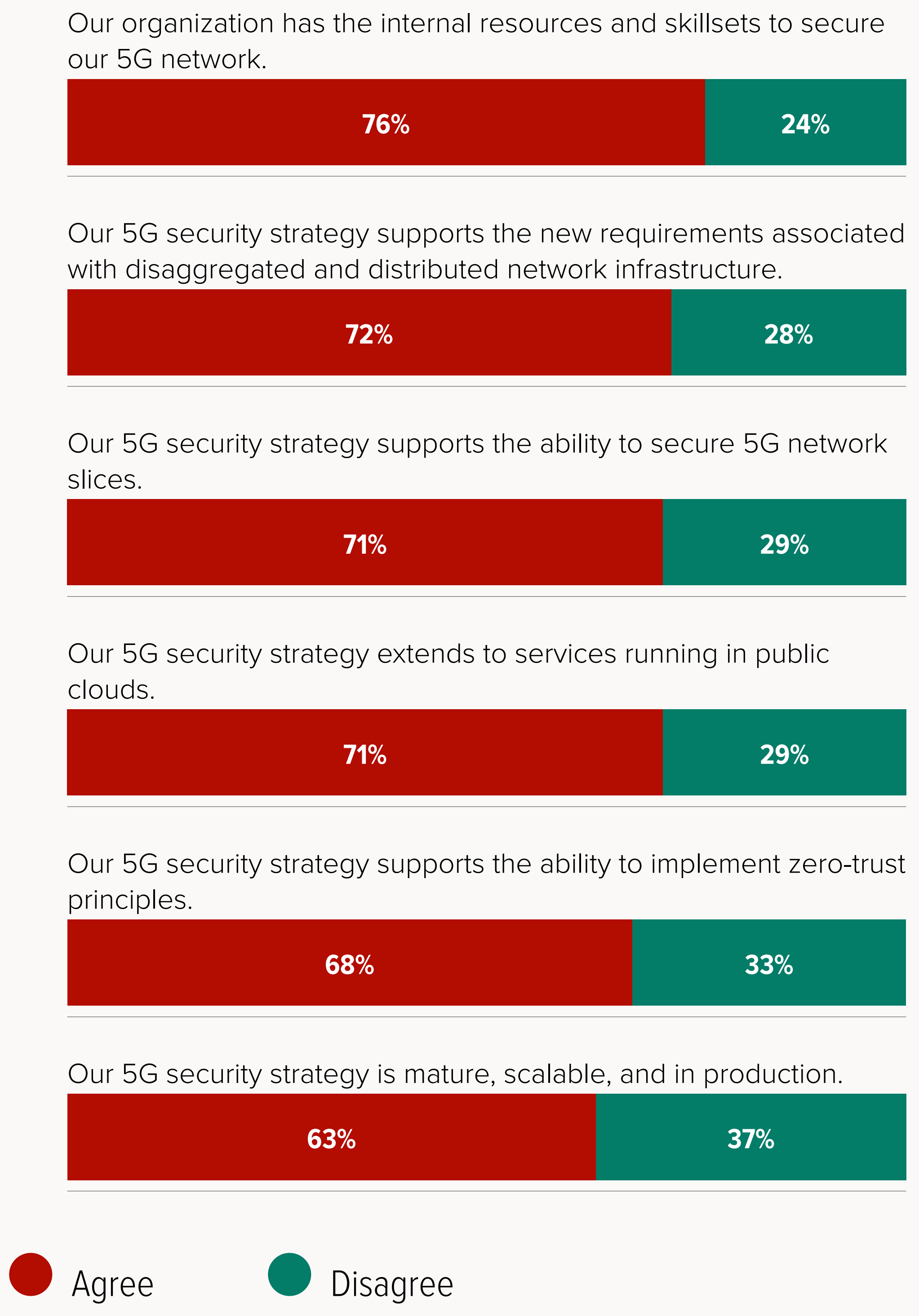
Figure 47:
As 5G emerges, with more edge activity and smart end-user devices, how does your organization plan to evolve its security strategy?



Since the launch of commercial 5G NSA took place in 2019, operators have had more than two years to prepare and execute their 5G security strategies. As **Figure 48** shows, approximately two years on, 63%–76% of operators believe that they have made considerable progress. For example, 63% of operators believe they have in place a mature and scalable security strategy that is equipped with the resources and skillsets (76%) to support the new requirements associated with distributed infrastructure (72%) and to secure 5G network slices (71%).

In addition, 68% agree that their security strategy supports the ability to implement zero-trust principles. This level of readiness was not unexpected, given 5G's broad appeal and reach, but one interesting data point was the higher than anticipated number of operators (71%) that agreed that their security strategies already extend to running services in public clouds, despite the limited number of commercial implementations.

Figure 48:
How important are the following capabilities for securing 5G infrastructure at your organization?



Red Hat

Executive Summary

You are only as secure as your weakest link. As application environments evolve, security teams are increasingly challenged to keep up with the changing risks, compliance requirements, tools, and architectural changes introduced by these innovations. Traditional perimeter-based network security is no longer effective on its own. Security should be implemented within each layer of the application and infrastructure stack. Automation is a critical part of scaling how the organization addresses security and compliance monitoring.

Red Hat wants to help you have confidence as you adopt a continuous security strategy to maintain security and regulatory compliance, while helping your business remain competitive, flexible, and adaptable. Red Hat provides telco-grade technologies to build, manage, and automate hybrid clouds more securely as part of a layered, defense-in-depth security strategy, and our broad partner ecosystem extends these capabilities even further. You can take advantage of the capabilities at each layer in your environment, including operating systems, container platforms, automation tools, Software-as-a-Service (SaaS) assets, and cloud services. Visit redhat.com/security to learn more about Red Hat's commitment to protecting your environments and the data and privacy of your customers.