RAD

Your Network's Edge®

Top 2022-2023 Trends in CSP IoT and Private 5G Campus Services

Table of Contents

Introduction and Key Findings

Introduction & Methodology

For Communication Service Providers (CSPs), IoT is a growth market. Service providers are beginning to develop and launch specific offerings for enterprises who are utilizing IoT as part of their core business, beyond the provision of simple data plans that enable network connectivity. Today's IoT touches every vertical from Healthcare to Manufacturing and Retail, as well as Public Utilities and Smart Cities. This is a powerful opportunity for CSPs.

This report is designed to get greater insight into how carriers are approaching IoT services. Which specific use cases are of interest, and what are their architecture and network plans for the various industries they address? How are carriers approaching sophisticated IoT challenges such as network differentiation? Do CSPs have an IoT strategy in place that complements the emergence of 5G services more widely?

The data from this survey uncovers trends and insights directly from CSPs themselves, shining a light on what service providers have achieved so far, and what their plans are for the next 18 months. For CSPs looking to approach the IoT domain, or deepen their foothold in this growing market, it's a must-read.

Methodology

To get more insight into the state of IoT for CSPs, we commissioned a survey of 220 Telecoms stakeholders from companies of more than 5,000 employees in the USA, Europe and APAC. Respondents are all Director level or higher, and work in Product Management, Network Architecture, Network Engineering, Planning, Technology, and Network Operations. All respondents work in IoT, Business Services or Managed Services. We did not speak to vendors or service integrators.

This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during Q4 2022. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

Key Findings

1 2023 is the year we see more from CSPs than IoT data plans alone

95% of service providers include IoT as part of their offering. The market is maturing fast, and 70% of our respondents now offer or have near-term plans to offer IoT cloud connectivity, with 57% providing service integration. The shift to move beyond simple IoT data plans, where Communication Service Providers (CSPs) enable IoT device connectivity over cellular networks via SIM cards, shows that service providers recognize the demand and opportunity to offer more sophisticated IoT managed services and network differentiation.

2 Telecom Service Providers are approaching IoT verticals with a broad focus

There is no one clear industry target when considering where to offer IoT services. Today, 55% of CSPs are targeting Healthcare, 50% looking to Industry and Manufacturing, and 43% making Retail a focus. Government, Energy, Transportation and Smart Cities are all a focus for more than a quarter of CSPs, as well. There is a widespread need for service provider support in IoT services, and no doors are being closed.

3 The results are in: IoT and 5G go hand in hand

50% say that their private 5G offering includes IoT managed services bundled with their campus network. This stands to reason as 5G enables scalable outdoor coverage, which has become a must in IoT installations. It also enables low-latency connectivity of AGVs/mobile robots and maintains service continuity during handovers. 5G is becoming the de-facto converged OT/IT campus network, aggregating all campus endpoints, including IoT devices.

4 Service providers plan to offer IoT networking and security differentiation

CSPs are getting ready for the growing IoT market, which includes a wide range of connected devices and applications, and need networking and security enhancements. 58% say they will use network slicing for IoT, while 52% are working on tools to enforce bounded latency and ultra-high network reliability. Bounded latency means that the latency isn't only low, but is also deterministic, i.e., it doesn't go above a certain threshold. This is required for real-time use cases such as control of industrial machinery, remote medical operations and VR/AR. 40% are building edge services through a hyperscaler while administering services by the CSP, and 56% are looking to expand security-as-a-service.

5 IoT gateways are critical to CSPs for aggregation and connectivity

97% of CSPs include IoT gateways in their private 4G/5G ecosystem, to bridge a range of interfaces and aggregate IoT devices to the WAN or private network. 49% of this cohort doing so to enable the integration of existing brownfield sensors to their 4G/5G network. Aside from cost, the top features of IoT gateways that service providers are looking for are all various network interfaces – WiFi AP support, LoRaWAN support and 5G uplink. Most CSPs opt for a single SKU (stock keeping unit) strategy, as this will limit complexity and cost by simplifying inventory, and make it easier for CSPs to serve a wide range of verticals and business use cases.

Survey Report Findings

Top Target Verticals for IoT Services

Communication service providers (CSPs) are addressing many different verticals. The top target verticals for IoT services are healthcare (55%), Industry and manufacturing (50%), and Retail (43%).

It's important to note that IoT has relevance across all of these industries and others besides, but these are the verticals where CSPs see an opportunity for their own growth. For example, Oil & Gas may be more likely to build their own solutions in-house, which could be the reason for their placement at the bottom of the list.

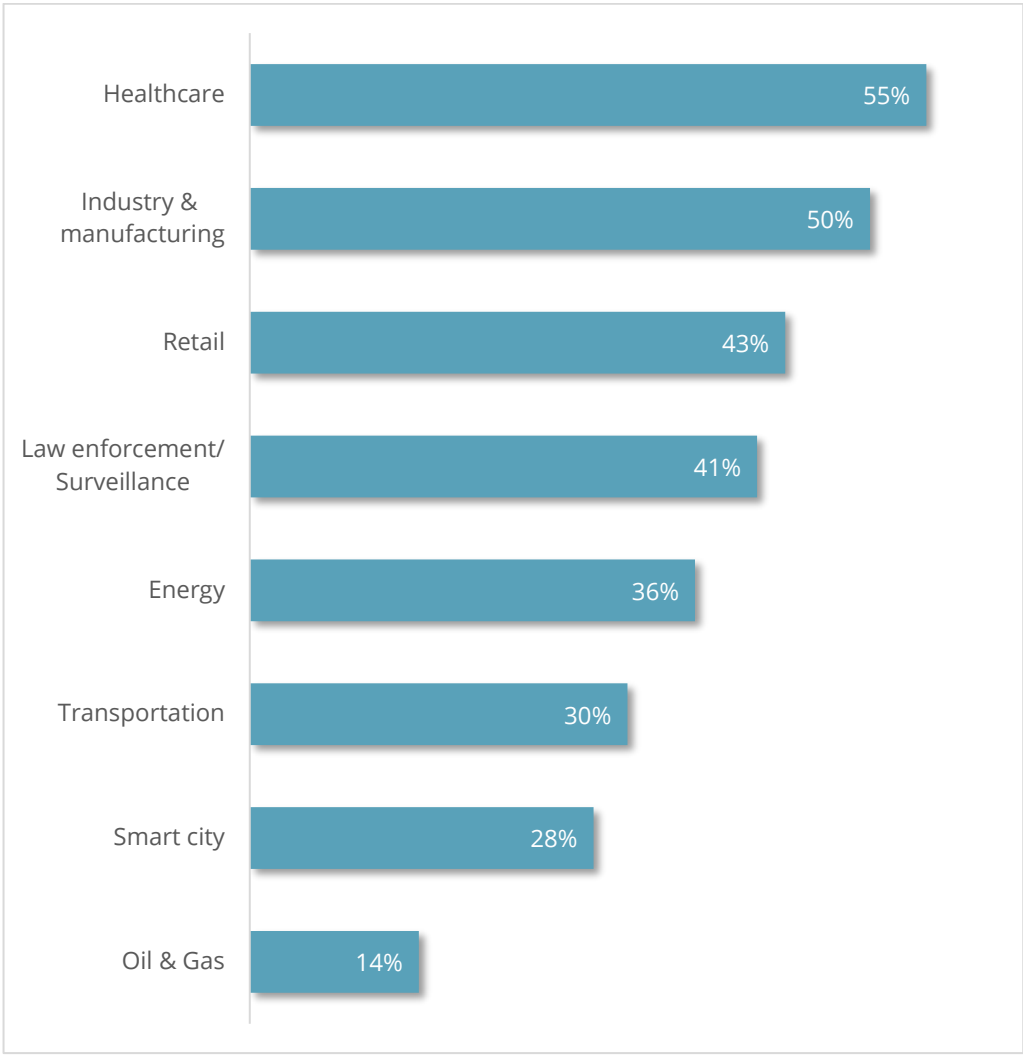

Figure 1: Top Target Verticals for IoT Services

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

IoT Services Provided, 2022-2024

95% of CSPs are offering IoT services.

We asked respondents to define what IoT services they provide, or have near-term plans to provide. 70% cite IoT cloud connectivity, which allows enterprises to seamlessly and securely connect low-power devices in their native protocols to IoT applications hosted on public clouds. 57% mention IoT integration services, and 43% provide IoT data plans, where CSPs enable IoT device connectivity over cellular networks via SIM cards.

CSPs have moved beyond offering simple data plans for IoT, and are looking to play a role in the entire IoT value chain. This means offering cloud connectivity services, hosting IoT applications, IoT Security-as-a-service, and providing IoT integration services in enterprise campuses.

It's clear that CSPs increasingly see themselves as IoT integrators and providers of IoT managed services, leveraging their customer base and network install and operational expertise.

CSPs are working with cloud hyperscalers to offer access to IoT applications, in the public cloud, in network edge locations and in private campuses.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

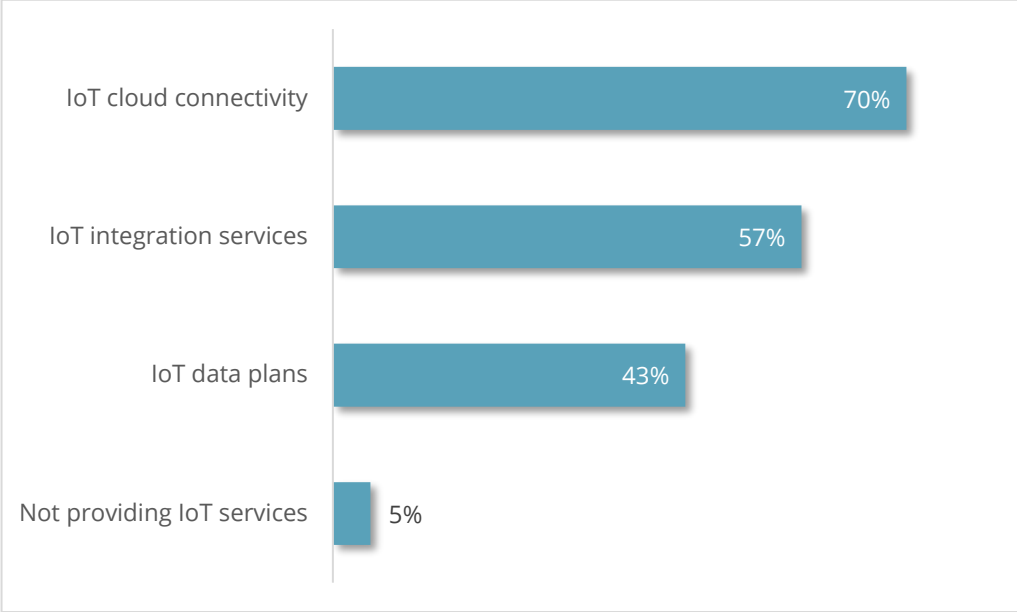

Figure 2: IoT integration services, 2022-2024

Inclusion of IoT Gateways in Private 4G/5G Offering

97% of respondents include IoT gateways as part of their overall private 4G/5G ecosystem. Of the 3% that don't currently include them, 2% are planning to do so.

Almost half (48.5%) cite the use of IoT gateways to aggregate existing brownfield sensors to a campus network & MEC, and 38.5% call out IoT gateways as a way to be future proof for future 5G network upgrades. 10% use IoT gateways to introduce network intelligence which is not available natively from the devices themselves.

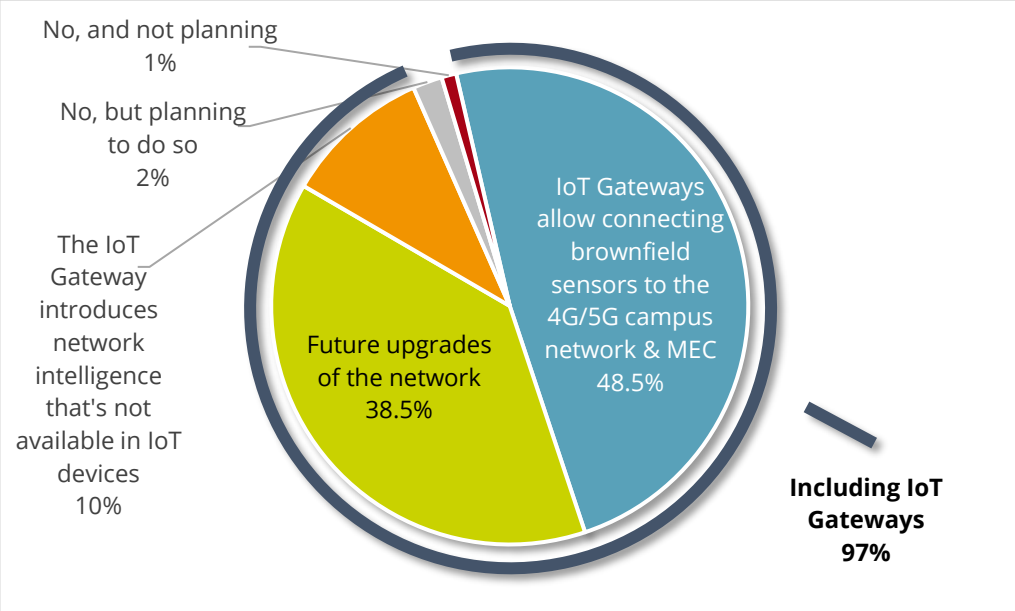

Figure 3: Inclusion of IoT Gateways in Private 4G/5G Offering

The Importance of Connecting Brownfield Sensors, by Target IoT Verticals

We looked deeper into the data of respondents who believe IoT gateways are important in the private network ecosystem specifically because of the capability to connect brownfield sensors.

Which verticals believe this is most critical?

Oil & Gas and Energy campuses were amongst the first to implement IoT, and so it stands to reason that they will have a substantial existing installed base of smart devices and sensors. It's therefore no surprise that they top the list, as they need these brownfield devices to be easily integrated into the transforming OT networks.

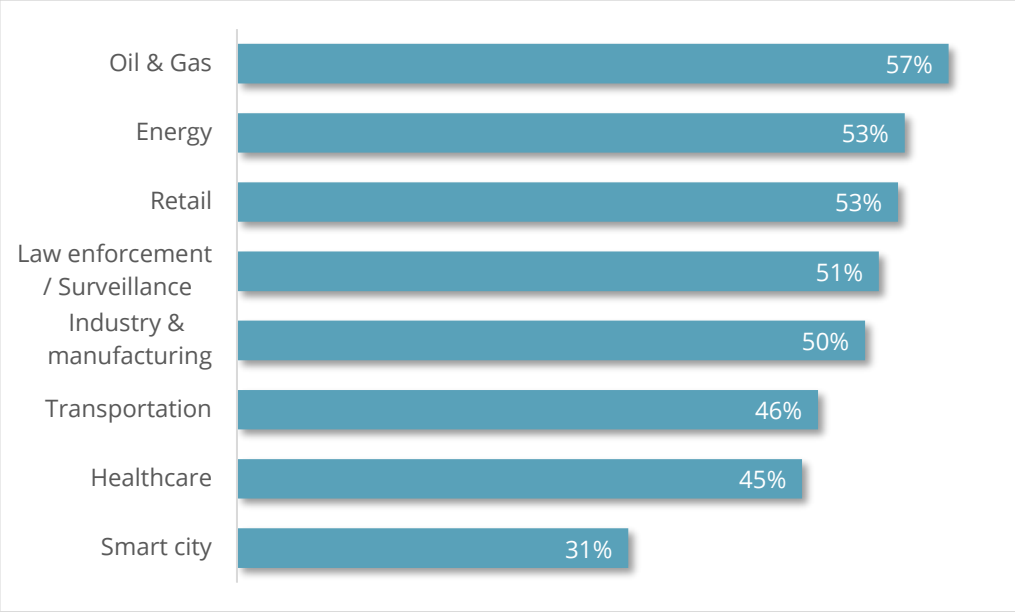

Figure 4: "IoT Gateways Allow Connecting Brownfield Sensors to the 4G/5G Campus Network & MEC", by Target IoT Verticals

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Bundling of Cloud Offering with IoT Services

CSPs are looking to complement their IoT offering with cloud and edge cloud services.

47% say they will provide IoT services off their network edge clouds.

39% say they will bundle IoT into their private 4G/5G offering, including offering services from the campus edge.

A further 14% will introduce cloud connect automation.

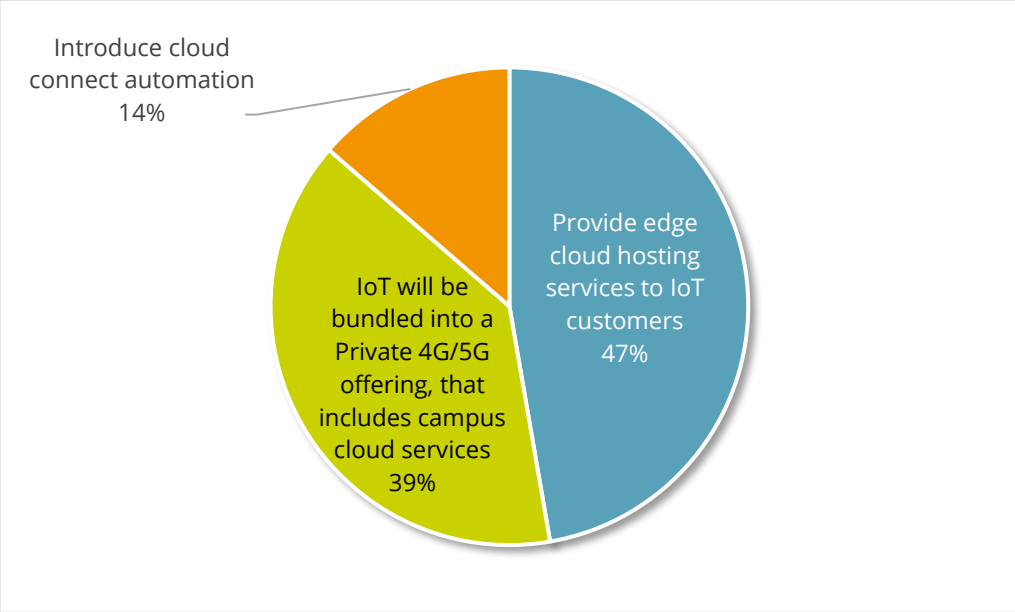

Figure 5: Bundling of Cloud Offering with IoT Services

Multi-Cloud & IoT Services

It's common for enterprise customers to have a multi-cloud environment, with different applications on different clouds. For service providers, offering multi-cloud connectivity should be an important consideration, both to serve end-users, and to offer differentiated services.

Two-thirds (66%) of respondents say multi-cloud access for IoT services is important. 31% have a neutral opinion, and 3% say multi-cloud access for IoT services is not very important (Figure 6). CSPs are currently beginning to offer IoT cloud connect services, while growing their relationships with the larger cloud providers. The results of the survey indicate that they aim to become multi-cloud connectivity "hubs" to offer value to their business and IoT customers. With this added value, customers may avoid the need to establish separate connectivity to each cloud provider.

Of the 66% who believe multi-cloud is important, we asked – why (Figure 7)? 38% cite IoT applications that reside on the cloud or edge clouds, 33% say IoT gateways aggregate multiple sensors or devices that need to access workloads in different clouds, such as public, edge and private. Another 29% confirm that their business customers' multi-cloud strategy dictates an IoT multi-cloud strategy.

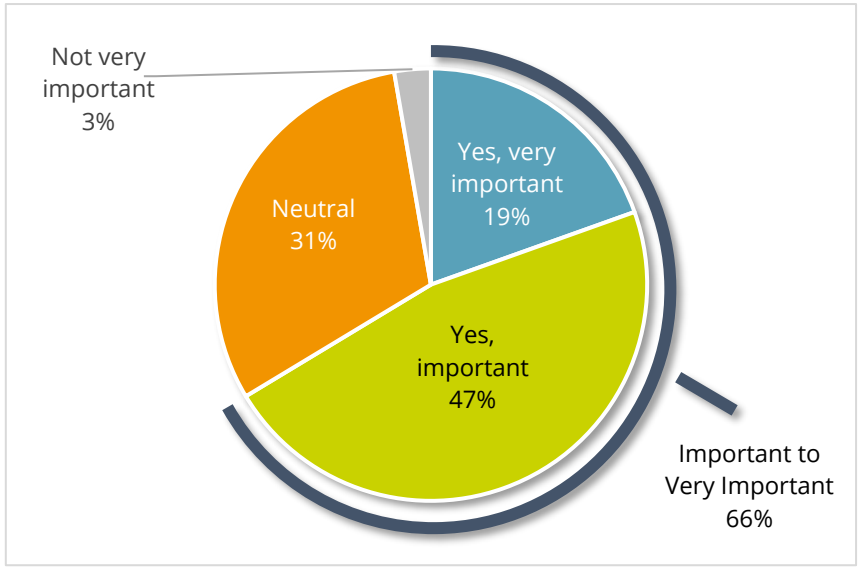

Figure 6: Importance of Multi-Cloud Access for IoT Services

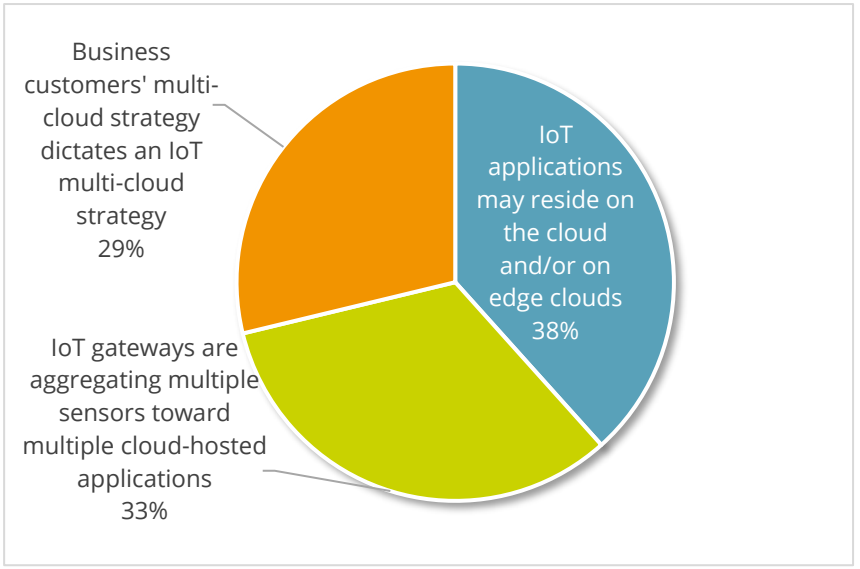

Figure 7: Why Multi-Cloud Access Is Important

Top Features of IoT Gateways

While cost will always be an important consideration, the following top three answers are WiFi AP support (39%), LoRaWAN support (36%) and 5G uplink (35%), all types of network connectivity interfaces.

It's clear that service providers want a variety of LAN and WAN interfaces on their IoT gateways to support the many connectivity options that are in use in the field.

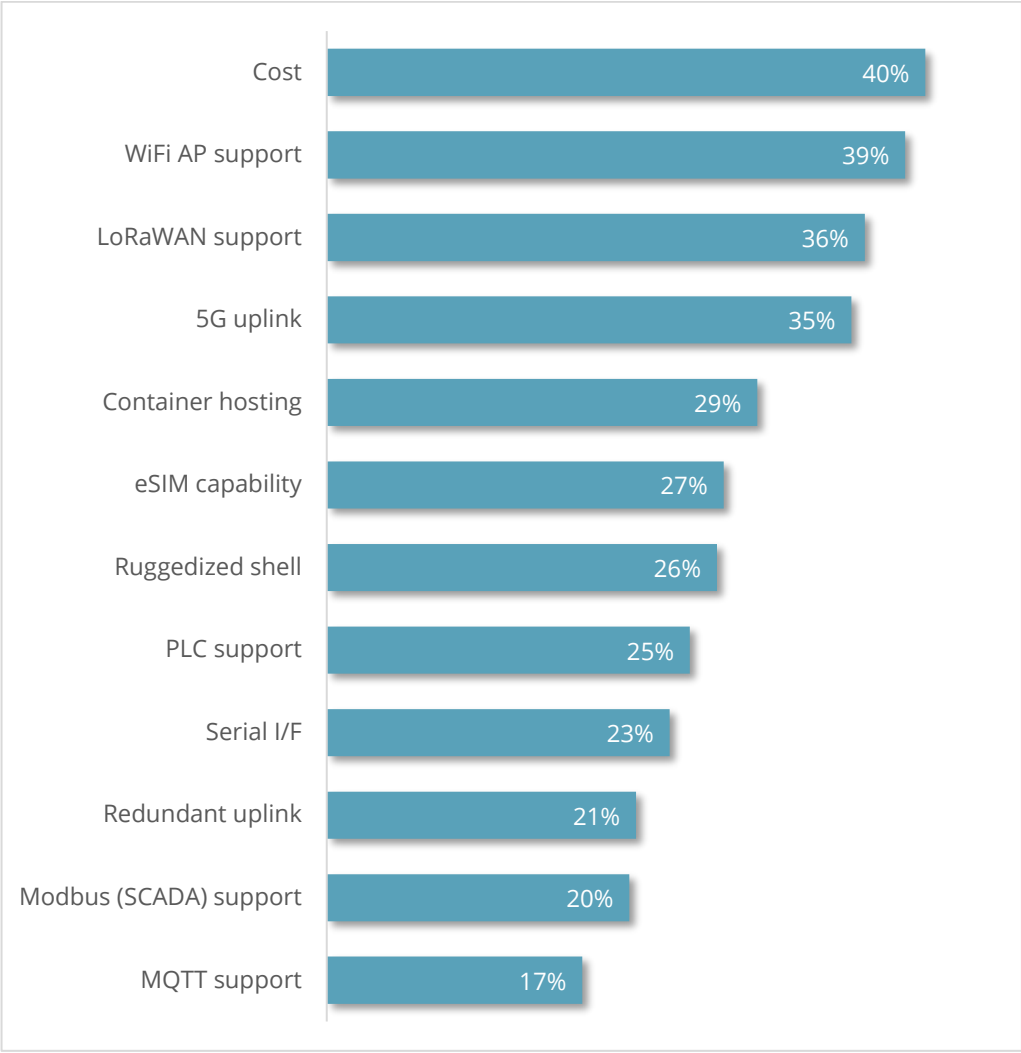

Figure 8: Top Features of IoT Gateways

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Varying Sensor/Machine Connectivity Requirements

We asked survey respondents how they plan to handle the varying sensor/machine connectivity requirements across different customers and verticals.

57% of respondents want to use a single SKU (stock keeping unit) strategy, in which CSPs use a single ordering option for feature-rich IoT gateways that fit all customer use cases, rather than a dedicated ordering option for each use case. This is one gateway which will serve multiple purposes. This makes sense, as service providers have so many verticals to serve, as we saw in Figure 1, and need to keep costs, inventory and operational complexity to a minimum.

23% of respondents say that they will create bespoke and tailor-made solutions for each customer need, and 20% will narrow down their use cases to concentrate on just a few.

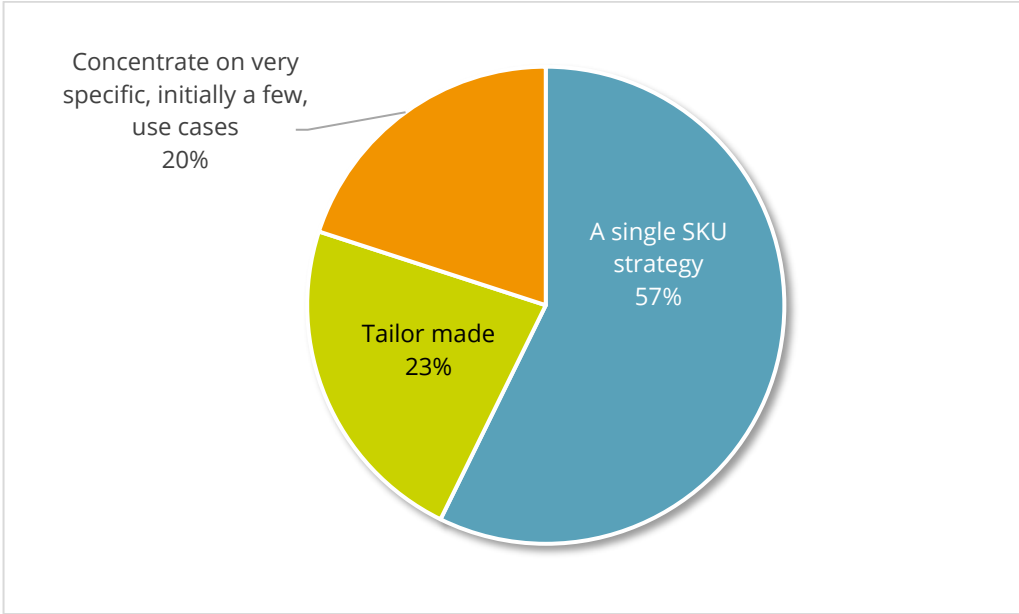

Figure 9: Varying Sensor/Machine Connectivity Requirements

Varying Sensor/Machine Connectivity Requirements, by Services and Offerings

We looked more closely at those who said they need a single SKU strategy (Figure 9), and can see that it's important for CSPs, no matter their involvement with the customer or how sophisticated their offering. 59% are offering cloud connectivity, 50% provide integration services, and 44% are offering IoT data plans (Figure 10).

CSPs are preparing themselves for different requirements, looking for an efficient inventory.

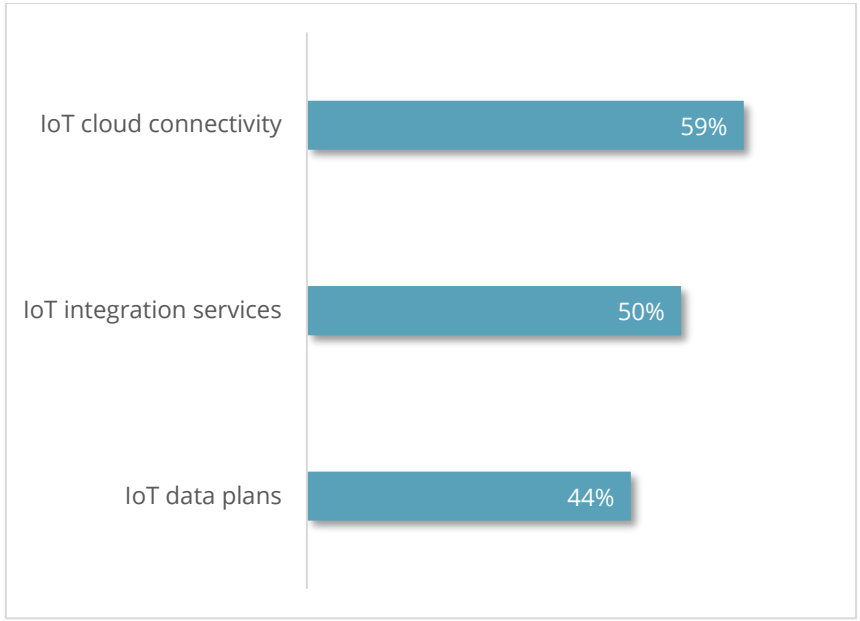

Figure 10: "A Single SKU Strategy", by IoT Services Provided

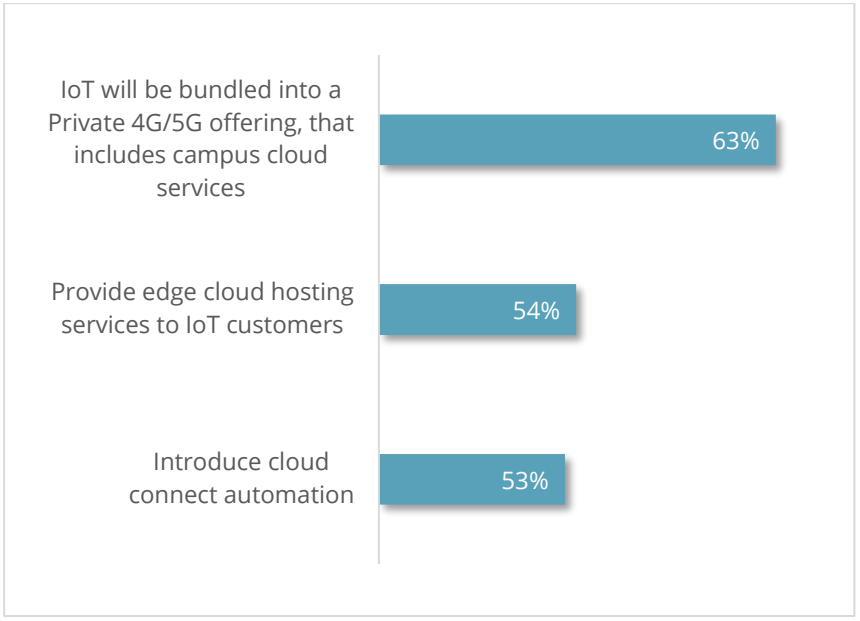

Figure 11: A Single SKU Strategy", by Bundling of Cloud Offering

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Typical Lead Time of Networking Appliances Vendors

When considering inventory plans and service rollouts, it's also important to think about how quickly CSPs can get the building blocks ready and be able to offer the service.

On average, we can see from the data that the typical lead time from networking appliance vendors is 21 weeks.

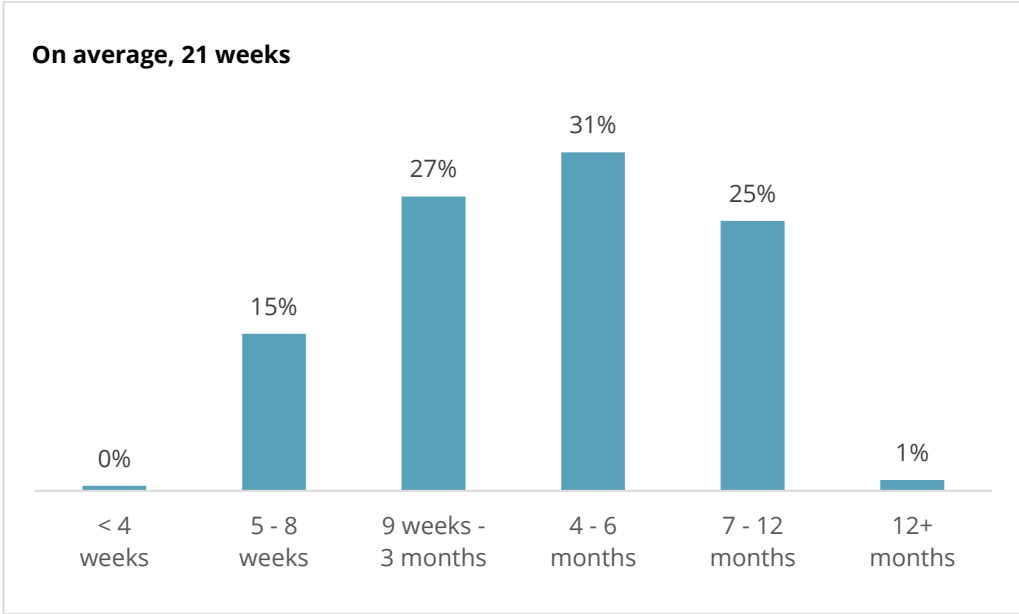

Figure 12: Typical Lead Time of Networking Appliances Vendors

*Percentages do not add up to 100% due to rounding up of numbers

Network Differentiation Tools to IoT Services

We asked CSPs if they are planning to apply network differentiation tools to IoT services, to properly accommodate different types of traffic, and if so – how?

From the responses, we can see how sophisticated the tools are being used to differentiate IoT traffic, and how CSPs are preparing themselves to the strict latency and reliability requirements of IoT applications. As a result, 58% of respondents say they will use dedicated network slices for IoT, which underscores the tight connection between IoT and 5G. In addition, 52% say they will enforce bounded latency and ultra-high network reliability onto IoT traffic. 30% say they will apply QoS to IoT services and 29% say they will backhaul IoT traffic on a dedicated NB-IoT/LTE-M RAN.

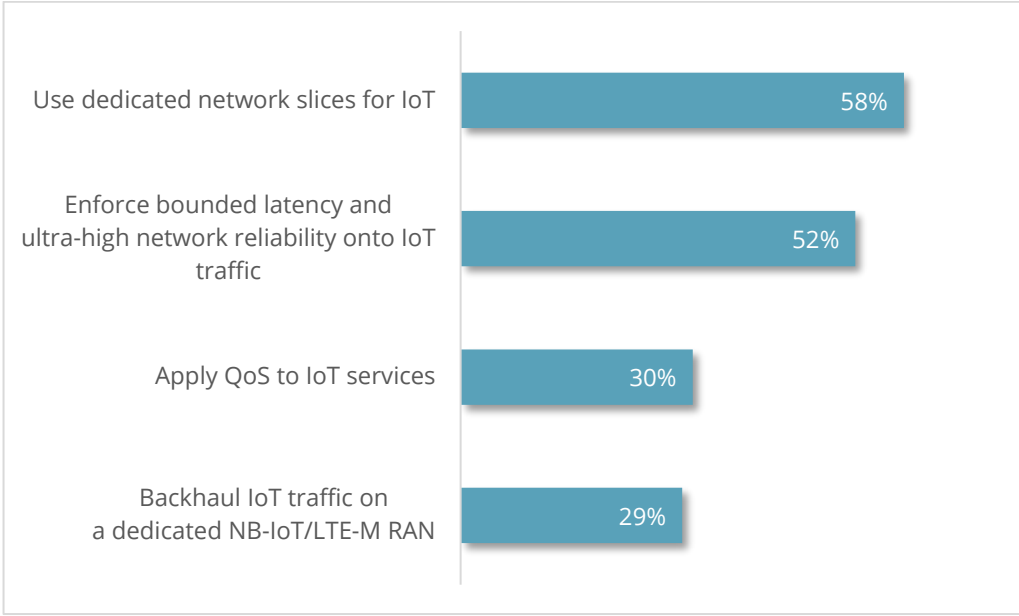

Figure 13: Network Differentiation Tools to IoT Services

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

5G's Role in Fixed Wireless Access Services

5G Fixed Wireless Access (FWA) is going to be a gamechanger for CSPs. In particular, more than half of respondents (56%) say that 5G FWA will allow them to extend their reach to previously unserved geographies using 5G FWA as the enabler.

26% say 5G FWA is an enabler for offering edge services, 15% say it is a replacement for wireline access services, and just 3% say it is not on their radar for 2023.

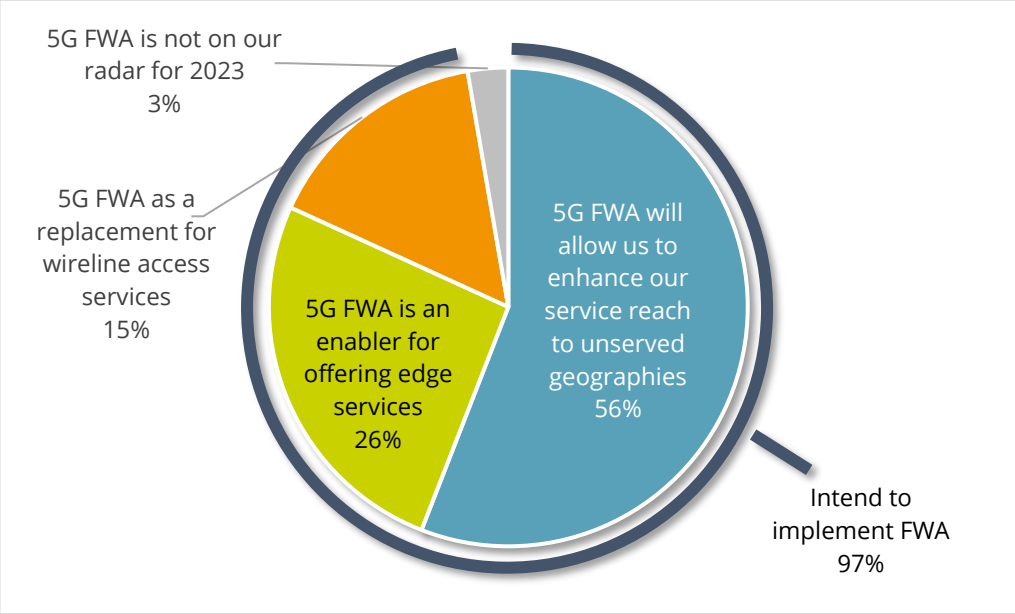

Figure 14: 5G's Role in Fixed Wireless Access Services

What's Included in Private 5G Offerings?

IoT and Private 5G are considered as enablers of industrial digitization**. 94% of CSPs plan to offer a private 5G service in 2023**, with just 6% putting it off. 15% offers a standalone 5G campus network and MEC.

50% of respondents say that their private 5G offering includes a standalone 5G campus network and MEC, bundled with managed IoT services, and 29% say their offering includes a hosted private 5G service (NPI-NPN).

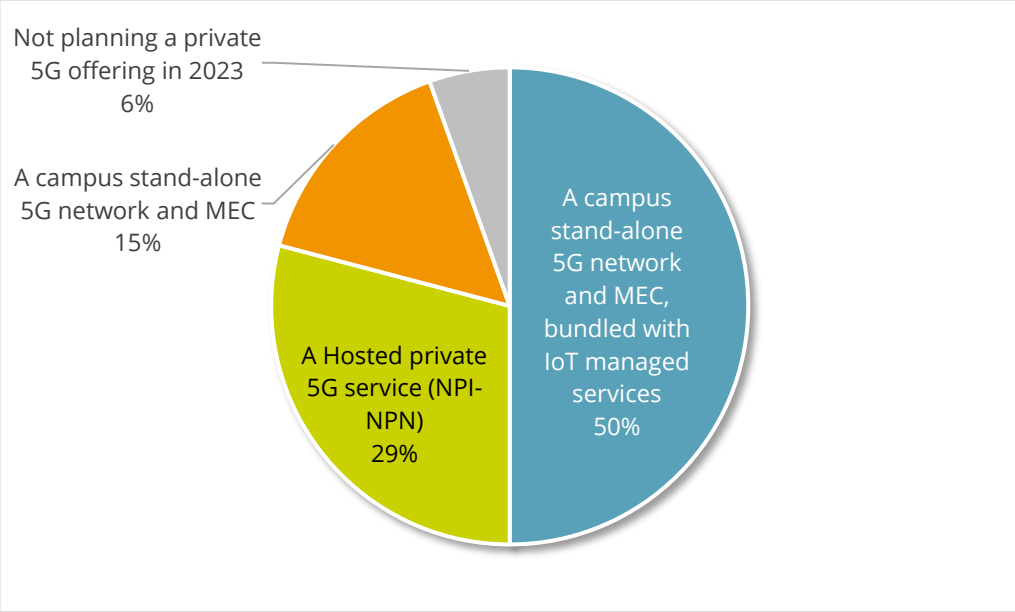

Figure 15: What's Included in Private 5G Offerings?

How Are Service Providers Building their Network's Edge?

We asked service providers to elaborate on how they are building the network edge.

76% of CSPs say that edge infrastructure will be built by hyperscalers, as they are better fit to provide a scalable cloud infrastructure. 64% of CSPs plan to offer edge hosting services to their customers. This is an indication that CSPs want to provide IoT managed services to support them in maintaining strong customer relationships.

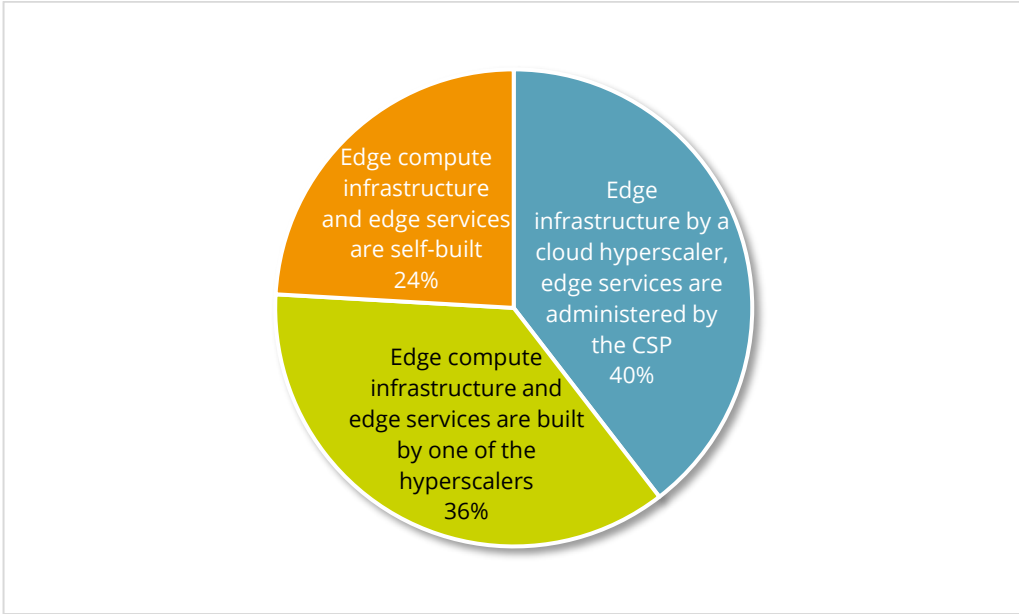

Figure 16: How Are Companies Building their Network's Edge?

Providing Security as a Service to Business Customers

We asked survey respondents if they provide security-as-a-service to their business customers. Service providers are keen to enhance their security services, especially with so many moving parts in the service delivery chain.

56% of respondents say they are looking to expand their security as a service offering, with just 27% citing that business customers rely on their own security solutions and hence are not ready to buy them from CSPs.

CSPs are looking for ways to move up the services value chain and effectively provide an alternative to on-premises enterprise and IoT security. As part of the strategy to make this happen, 50% say they host zero-trust network access services, 35% say they provide DDoS protection service, and 30% say they provide firewall-as-a-service.

In IoT, where devices are easily compromised and can be used to gain a foothold to a wider network, security is more critical than ever.

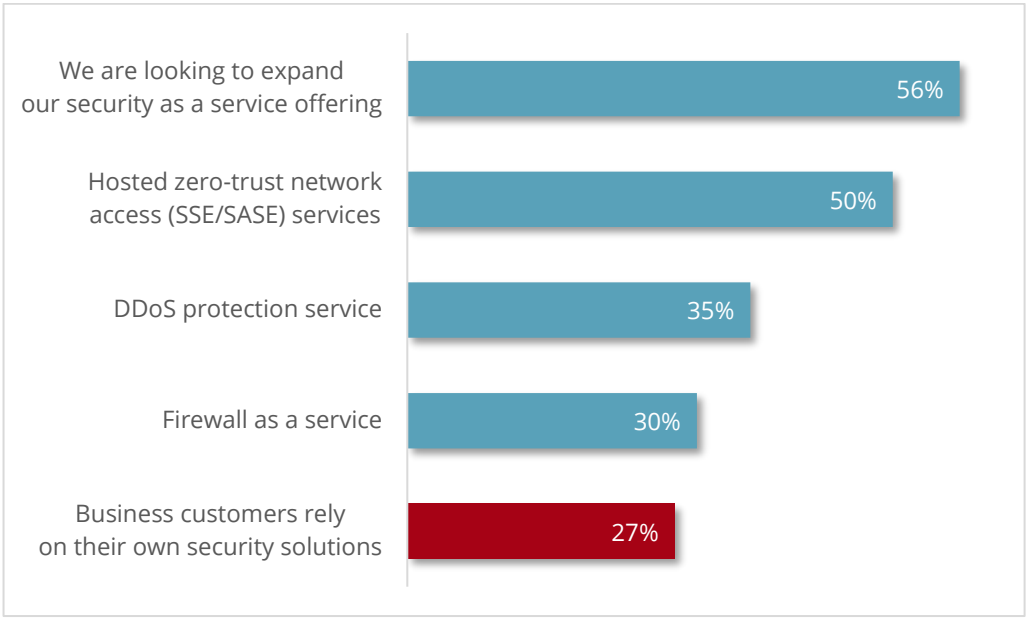

Figure 17: Providing Security as a Service to Business Customers

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Demographics

Country, Company Size, Job Seniority, Area of Responsibility, Role

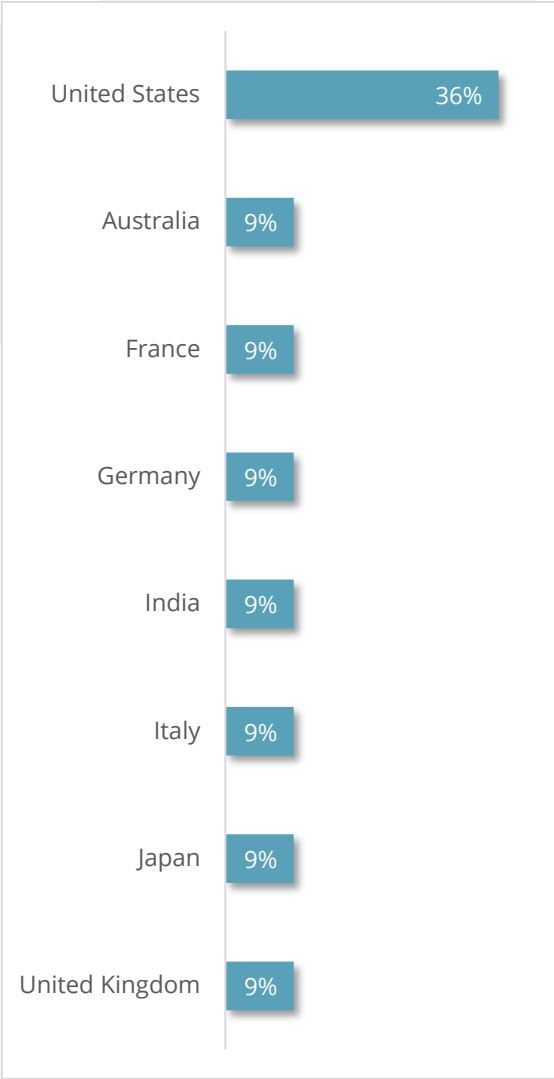

Figure 20: Country

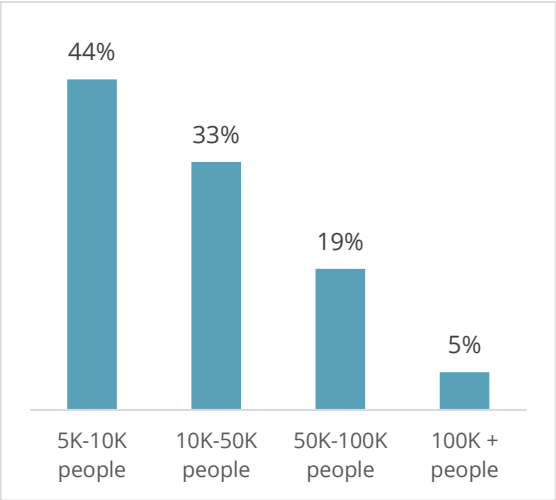

Figure 188: Company Size

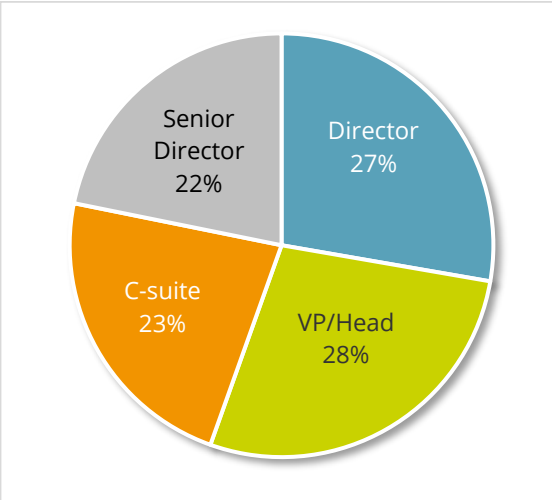

Figure 19: Job Seniority

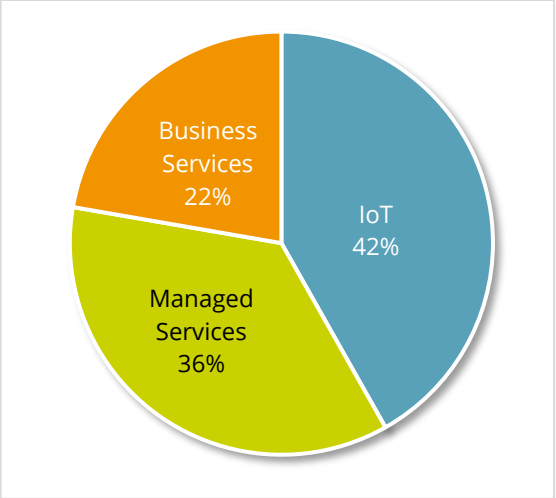

Figure 19: Area of Responsibility

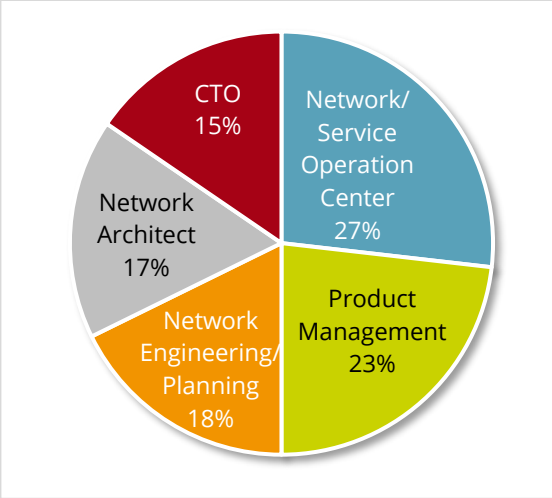

Figure 20: Role

About RAD

RAD delivers best-of-breed edge, xHaul and Industrial IoT solutions for communications service providers and critical infrastructure operators. Drawing on over 40 years of innovation and expertise, RAD works closely with customers to design market-leading solutions that simplify operations, help users derive more value from their networks and ensure always-on reliability. Whether for carrier edge business services, 5G fixed wireless access, Private 5G (campus-based edge cloud) for IoT services, or O-RAN xHaul, RAD supports customers through the entire project lifecycle, from design to deployment. Founded in 1981, RAD serves as the anchor of the $1.8 billion RAD Group.

Contact us

For more information, please visit us:




Email: market@rad.com