Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING CUSTOM REPORTS

Heavy Reading's 2019 5G Security Survey

A Custom Research Report Produced for F5 Networks, Fortinet, NetNumber, and Palo Alto Networks

AUTHOR: JIM HODGES, PRINCIPAL ANALYST, HEAVY READING

TABLE OF CONTENTS

1. INTRODUCTION AND KEY FINDINGS

5G is fundamentally reshaping the basic design constructs that communications service providers (CSPs) utilize to deliver services on their networks. One area that is particularly daunting and subject to flux are the requirements associated with the creation of a secure operating environment.

This report presents in detail the key findings of a recently completed market research study examining how CSPs are coming to terms with 5G security challenges and documents their implementation strategies and use case preferences.

1.1 Key Findings

5G Security Use Case Priorities: Trial vs. Commercial Launch

Before commercial deployments began, 5G security pilot trial activity focused on two key areas: narrowband Internet of Things (NB-IoT) and edge cloud security. NB-IoT security (including random access network [RAN] monitoring) resonated with 59% of respondents, as did addressing the general topic of edge cloud security (57%). Other areas of interest were per-slice security (40%) and signaling security on roaming networks (32%).

While survey respondents from the United States (U.S.) and Rest of World (RoW) agreed on the priority ranking of edge cloud security as a top trial priority, RoW respondents had a greater trial focus on NB-IoT than U.S. respondents (72% vs. 43%). In contrast, U.S. respondents were more interested in conducting per-slice security trials than RoW respondents (50% vs. 32%).

Despite trial interest, IoT translates into an initial lower *commerical* security use case priority than core and RAN-related security use cases. Within these, the top three priorities are core network signaling (47%), cloud RAN fronthaul and backhaul security (44%), and core network security services (35%). Security services for mobile edge computing (MEC) and the IoT scored in the 20% to 28% range in the context of launch priority. The message here is that CSPs' initial focus is on deploying security capabilities that will address their immediate security challenges inherent with the introdution of the 5G New Radio (NR) and Next-Generation Core (NGC).

5G Security Investment and Monetization Strategies

Sixty-three percent of respondents believe that 5G will disrupt service delivery models. While this will inject complexity into security service delivery, the upside is that the survey respondents also see additional business opportunities. For example, 95% of respondents agree that 5G will result in a greater focus on business-to-business (B2B) service delivery, while 76% agree the same is true in a business-to-consumer (B2C) context.

Another reason CSPs are focusing on the RAN and core is that they believe it will drive significant security revenue. Within 3 to 5 years, 27% of respondents expect cloud RAN security to achieve more than 20% annual growth. Core security services and core network configuration services attained third- and fourth-place scoring (22% and 21%) in this same growth category. The second-place ranking of enterprise mobility security

services (25%) among the top annual growth earners reinforces just how strategically important the delivery of cloud-based enterprise mobility managed security services has become in a relatively short period of time.

One factor for the revenue optimism is that CSPs are more focused on differentiating 5G security services through scale than pricing. For example, 53% of respondents chose scale, while only 20% chose price to differentiate their control plane signaling services. As a result, scale is also a consideration when selecting security vendors.

CSPs believe a number of functions are central to enhancing their 5G security-as-a-service (SECaaS) portfolio. The top priorities based on "extremely important" responses are application visibility for IoT services (40%), followed closely by international mobile subscriber identity (IMSI) correlation and secure applications on the mobile edge (both 38%), then automated cloud security (36%) and International Mobile Equipment Identity (IMEI) threat correlation (35%).

Greater revenue growth potential translates into greater investment, but CSPs are also mindful that the impact of strategic services must be factored into their network investment plans. For example, looking out 3 to 5 years, 31% of respondents believe that cloud RAN security will consume 5% to 10% of their 5G capital expenditure (CAPEX) spending, while 25% of respondents forecasted core network signaling would consume that amount of CAPEX and IoT security services garnered 23% to 24% response rates, which Heavy Reading believes points to the long-term strategic nature of IoT services. A significant range of respondents (16% to 24%) are still unsure of their investment priorities, suggesting CAPEX allocation for 5G security services remains relatively fluid.

Regardless of the core focus and early trial interest by some parties, less than a third of respondents (23% to 30%) plan to invest in slice-related security capabilities before commercial launch. There are a number of factors driving this, but one important consideration is the decision of whether to launch 5G utilizing the non-standalone (NSA – 5G RAN and 4G Core) or the standalone (SA – 5G RAN and 5G Core) architecture. If the NSA core is used for launch, then limited slicing capabilities can be supported.

Implementing the 5G Security Architecture

More than half of CSPs (55% to 65%) plan to launch security use cases utilizing the NSA option. This partially explains why there is a muted focus on securing slices and such a strong focus on cloud RAN security (65%) and core network signaling capabilities (63%), which must be addressed in either configuration.

Ninety-six percent of respondents advocate encryption on all layers of the networks. While support is overwhelming, several encryption options are being considered. Of these, the one with the greatest level of support in the radio network is Internet Protocol Security (IPSec) (54%) encryption. The other two layers of the networks, specifically the core and the edge/internet interface, also preferred IPSec, but with lower response preference rates (43% and 41%). The second most preferred approach was to secure these network layers using Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) options. These options received scores in the 25% to 34% range.

Control Plane Considerations

The signaling control plane of CSPs' current networks are extremely stable and secure. While 39% of the respondents recorded essentially zero instances of service impacting outages per month, 34% encountered 1 to 2 service affecting instances per month. This translates into 73% of CSPs having zero or 1 to 2 service impacting outages per month.

But these same CSPs are less confident that this level of security performance can be duplicated on the 5G control plane. Typically, about half of the respondents (42% to 55%) are "confident" in their abilities to secure the 5G control plane. Disappointingly, "extremely confident" responses fall only in the 9% to 29% range. But what is perhaps most disconcerting is the relatively high rate of "somewhat confident" and "not confident" responses. Aggregating these two responses rates translates into as many as 4 out of 10 CSPs having limited or zero confidence in their ability to secure strategically important 5G IoT-, MEC-, or application programming interface (API)-based security use cases.

One reason for this lack of confidence is that CSPs have come to the realization that the 5G control plane will be more complex to secure and more vulnerable to attack and fraud. For instance, 70% of respondents believe 5G roaming will be more difficult to secure (70%) and more susceptible to fraud (63%). Additionally, they agree that NR and NGC signaling storms will be more common (65% and 60%).

In response, CSPs are focusing on protecting against multiprotocol attacks through the implementation of distributed signaling firewalls. These can mitigate topology, hiding challenges and improving responses to calling line identifier (CLI) spoofing and robocalling threat vectors.

CSPs' signaling firewall deployment strategies must not only address 5G, they must also address the realities of managing and interworking a hybrid 3G/4G/5G control plane. In terms of protocol interworking, the respondent's priorities were HTTP2 – Diameter interworking (43%), HTTP2 – Session Initiation Protocol (SIP) interworking (38%) and then fraud/correlation capabilities (30%), and HTTP2 – SS7 interworking (29%), which confirms that HTTP2 must interwork with all established protocols.

In addition to signaling firewalls, other capabilities will also play a vital role in securing the 5G control plane. Of these, the network repository function (NRF) is most likely to be implemented at commercial launch (39%), while the network exposure function (NEF) was also seen as a commercial priority (33%). Tied for third place (24%) were the Security Edge Protection Proxy (SEPP), which secures roaming at the edge, and the 5G signaling firewall. Furthermore, while it is still "early days" machine learning-based automated provisioning and policy enforcement attracted significant commercial launch support (19%).

Threat and Fraud Mitigation

CSPs are considering a number of options to manage threats. Although using automatic threat redirection to send malicious traffic to a scrubbing center had the greatest level of support by the respondents (34% to 46%), other respondents are split on which other alternative to use. The second camp, which attained higher scores on the top end, favored the more comprehensive and automatic inline scanning approach (16% to 37%), while a third group advocating the most basic manual redirection approach fell into the lower 12% to 20% range.

CSPs plan to deploy a number of capabilities to address fraud-related challenges. Based on "extremely important" responses, 37% of respondents support the use of real-time fraud tools. Other capabilities, such as enhancing polling and call detail record (CDR) creation (31%), while list support (31%) and even IMSI/global title translation (GTT) correlation (28%) also had significant support.

Automation and Other Advanced Capabilities

Automated security policy is strategically important. The most common sentiment among the respondents (with a higher support by U.S. respondents) was that CSPs would launch commercial 5G services using manual policy and adopt automation over time (29%). In contrast, an almost equally sized second group (25%) plans to launch 5G with automated security policy without hiring additional staff. The third group (22%) also plans to launch 5G using automated policy but plans to hire additional staff. Based on second and third response rates, almost half of the respondents (47%) are committed to implementing automated security policy.

Operating expenditure (OPEX) reduction is a key factor influencing the decision to adopt automated security policy. While half of the respondents (49% to 53%) believe that automated policy will reduce OPEX at a level of 10% to 25%, a second group (27% to 31%) adopts the most pragmatic approach and gauges OPEX savings in the less than 10% range. The third group, representing 20% to 24% of respondents, adopts the most aggressive stance, forecasting an OPEX reduction of more than 25%. Combining the two upper scoring groups results in about 70% of respondents forecasting at least a 10% OPEX reduction.

Many CSPs plan to implement full content inspection in the 5G network. Support is strongest in the RAN and core where 42% and 41% of respondents appraised this capability as "extremely important." While the percentage of "extremely important" response levels dropped off for roaming (32%), implementing on the Gi-LAN (25%), and with MEC (24%) responses, the strong proportion of "important" responses for these three (49%, 42%, and 51%, respectively), validates that full content inspection is a valuable threat mitigation tool for a broad number of use cases.

Selecting 5G Security Vendors

The top three factors CSPs consider as "extremely important" when selecting security vendors are backward compatibility (39%), third-party integration certification (25%), and portfolio breadth and maturity (24%). Interestingly, existing vendor footprint was last on the list (15%), which suggests CSPs are open to working with new vendors if they meet the top three criteria. While U.S. and RoW respondents shared similar views, U.S. respondents put less weight on third-party integration certification than their RoW counterparts.

The two factors that respondents considered as "extremely important" when selecting fraud and signaling vendor solutions are programmable rule set support (41%) and multi-tenant use case support (39%). Other attributes, such as scale (31%), API/representational state transfer (REST) support (29%), and distributed architecture design (29%), matter as well. The message from this input is clear: signaling and fraud solutions must be programmable and scalable, multi-tenanted, and API-controllable to meet the real-time needs of distributed architecture configurations.

2. SURVEY DEMOGRAPHICS SUMMARY

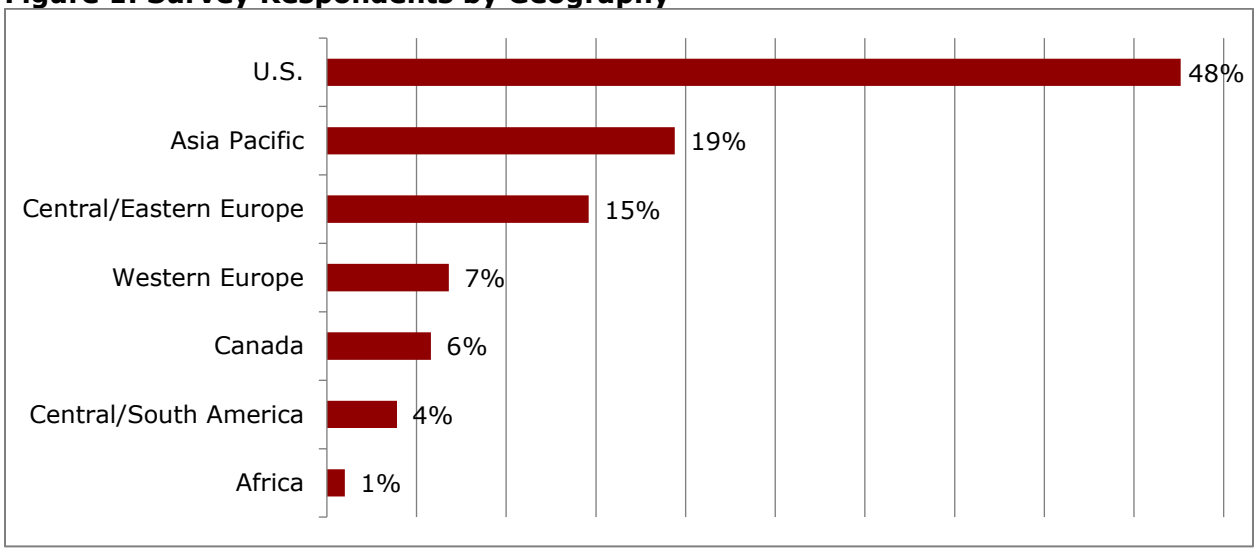
This research report is based on a comprehensive online survey launched in 1Q 2019. The survey created by Heavy Reading in collaboration with research sponsors, F5 Networks, Fortinet, NetNumber, and Palo Alto Networks was distributed by email to Light Reading's global list of service provider employees.

These respondents were invited to take the survey on the understanding of anonymity (i.e., that their names, job titles, and employers would not be made available to the study's sponsors or eventual readers), and that the results will only be presented in aggregate form. Respondents were not told which suppliers sponsored the study.

The survey contained a total of 28 questions and was promoted to attract a large base of high value respondents. As shown in **Figure 1**, a global mix of 103 qualified CSP respondents took the survey. Non-qualified, non-CSP responses were deleted. The largest employee sample was from the U.S. (48%), followed by Asia Pacific (19%), Central/Eastern Europe (15%), Western Europe (7%), Canada (6%), Central/South America (4%), and Africa (1%).

Given the distribution, the survey data was filtered using two categories: U.S. responses and those from the RoW. This was done to understand on a more granular basis geographic-specific trends between the U.S., which is aggressively rolling out 5G, and other countries, which may be adopting a more measured approach. For purposes of brevity, only significant variances in response trends between these two groups are noted in the main body of this report. Filtered group data for each question is provided in table format in **Appendix A**.

Figure 1: Survey Respondents by Geography

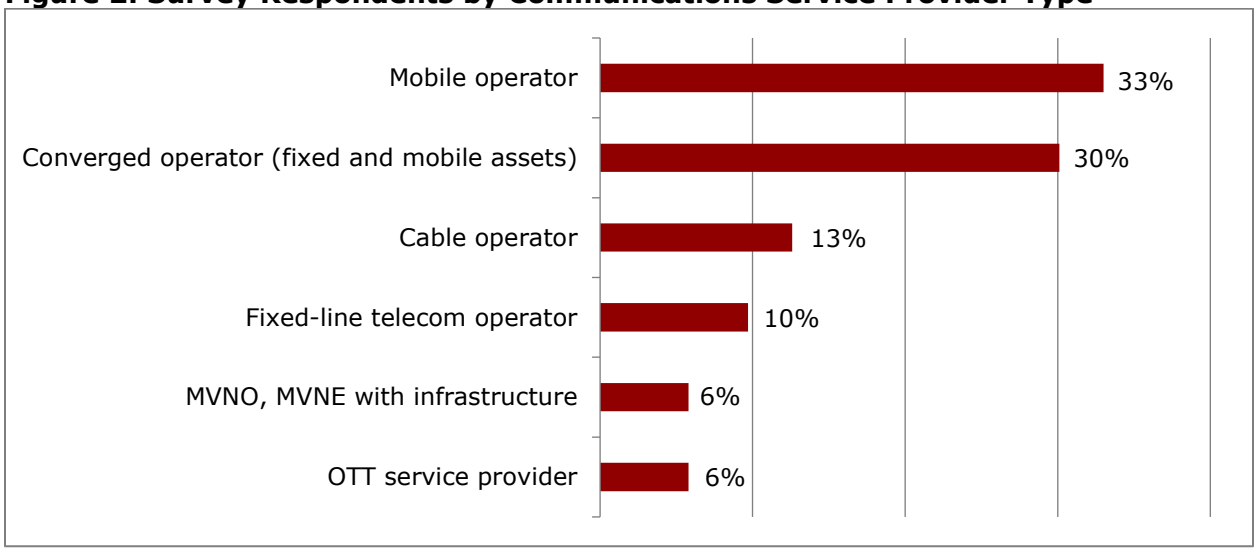


Question: Where is your company located? (N=103)
Source: Heavy Reading

The survey also attracted a broad range of CSP types and sizes, which provides a balanced view of overall 5G security strategies, given that 5G is germane essentially to all operators, including even over-the-top (OTT) and cable providers.

Of these, as shown in **Figure 2**, the two largest groups represented were mobile operators (33%) and converged operators (30%), which was not unexpected, given that mobile operators have a strong focus on upgrading existing mobile broadband services, while converged operators are looking not only at the mobile side of their business, but also at how to leverage 5G as a high speed fixed broadband access alternative.

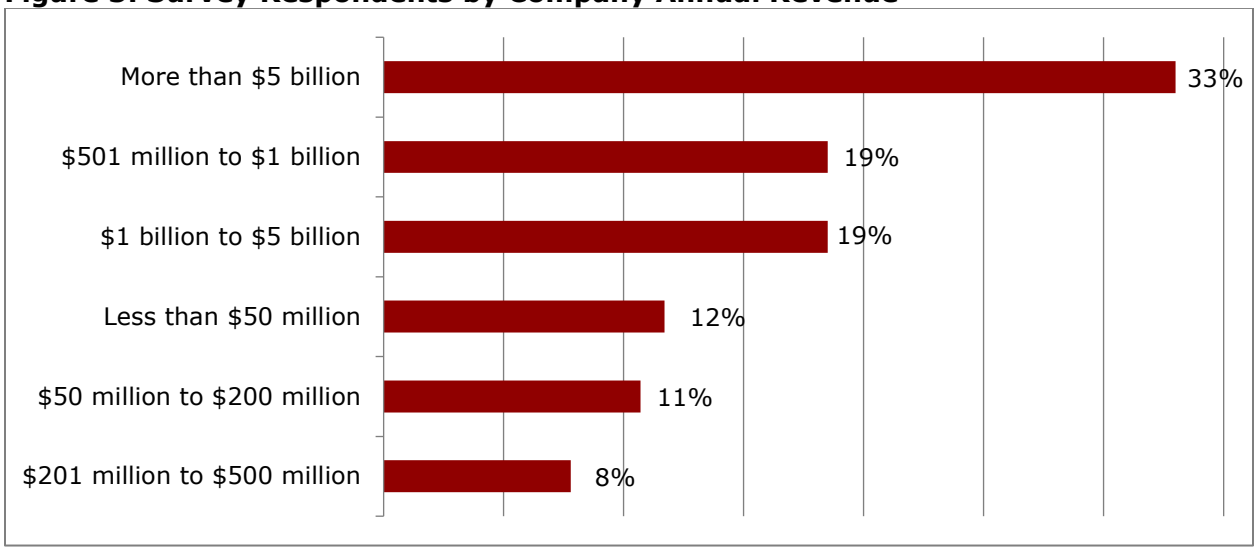
Figure 2: Survey Respondents by Communications Service Provider Type



Question: What type of communications service provider (CSP) do you work for? (N=103)
Source: Heavy Reading

As shown in **Figure 3**, 71% of the respondents worked for CSPs that generated more than $1 billion of revenue on an annual basis (33% + 19% + 19%), while 31% (12% + 11% + 8%) generated lower annual revenue ($500 million or less).

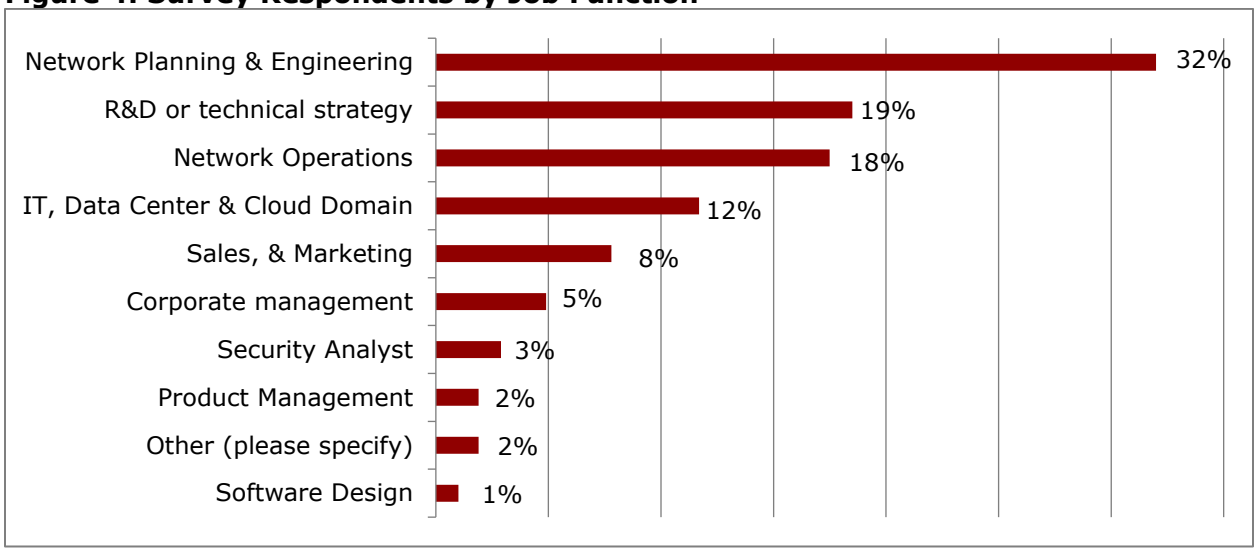
Figure 3: Survey Respondents by Company Annual Revenue



Question: What is your company's annual revenue? (N=103)
Source: Heavy Reading

Survey respondents, as shown in **Figure 4**, also tended to perform diverse roles in their organizations, including senior corporate management, research and development (R&D), network planning, network operations, IT data center and cloud, finance and sales, and marketing. The level of representation of respondents from network planning and engineering (32%), R&D (19%), and network operations (18%) is considered optimal because these respondents are ideally positioned to implement or plan the implementation of 5G and possess a pragmatic view of what it takes to secure the control plan and the user plane.

Figure 4: Survey Respondents by Job Function



Question: What is your primary job function? (N=103)
Source: Heavy Reading

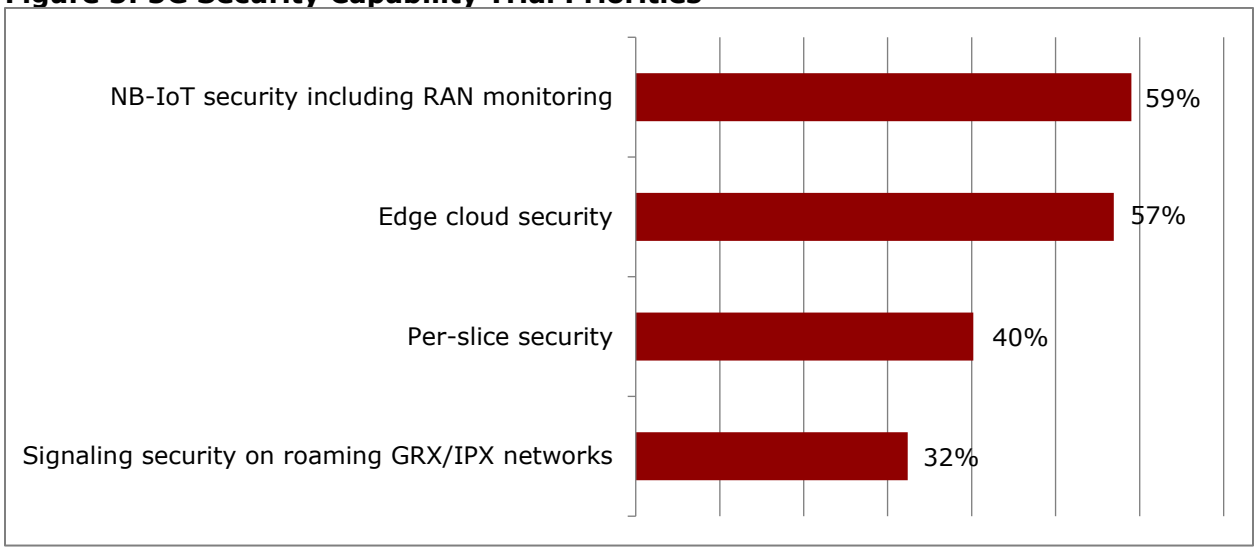
3. 5G SECURITY USE CASE PRIORITIES

Before any new mobile technology can be implemented commercially, it must be vetted in trials. A disruptive technology like 5G is no exception. The difference this time around is that the use cases and security focus areas are unique due to the impacts of new capabilities, such as network slicing and the ability to implement 5G in a distributed edge configuration.

In order to understand CSP 5G security strategies, the survey first concentrated on trial activity asking survey respondents to prioritize specific security trial focus areas. In this case, as **Figure 5** shows, of the four options presented, the two top priorities are NB-IoT security (59%) and edge cloud security (57%), followed by per-slice security (40%) and signaling security on roaming networks (32%).

The scoring of these attributes is logical, given that the edge cloud is a fundamental enabler for new services, such as NB-IoT. The interest in per-slice security is driven by the fact that it represents a new approach to security and policy enforcement that service providers must understand and feel confident they can secure before they commercially launch slice-based security services.

Figure 5: 5G Security Capability Trial Priorities



Question: Which security capabilities will you focus on during 5G pilot trails (select all that apply)? (N=101)
Source: Heavy Reading

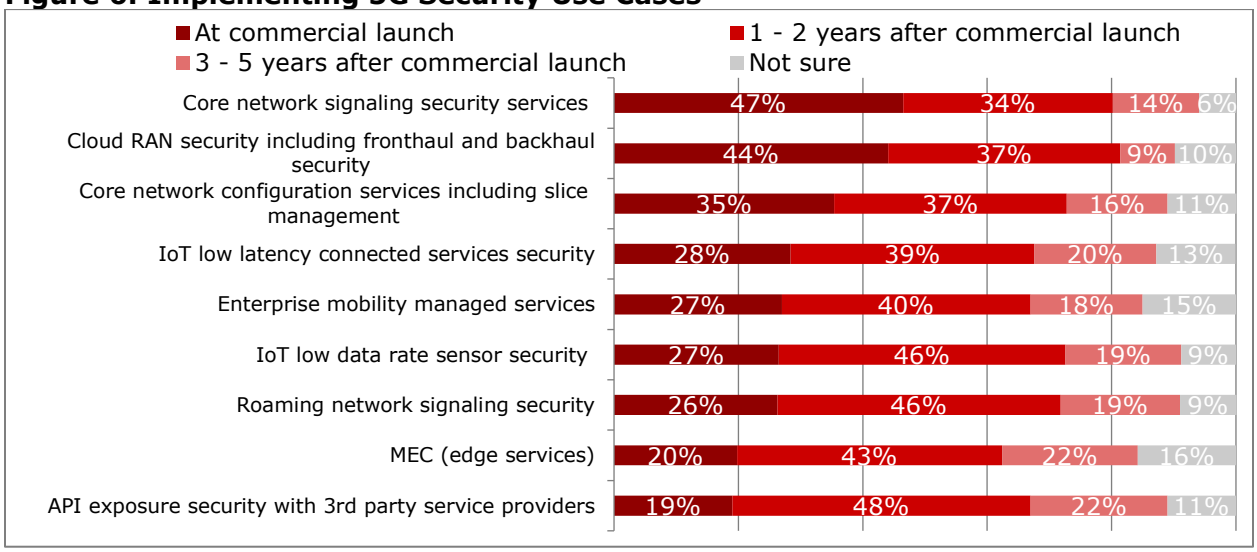
The introduction of 5G NGC and NR has major security implications due to the implementation of a fully separate control and user plane, as well as a fully distributed radio architecture.

In response, CSPs must reconsider how they deliver a complete suite of security services that encompass signaling security, enterprise security services, and even IoT and MEC services. In order to optimize data analysis, a common set of nine 5G security use cases was developed and used in a number of questions.

As shown in **Figure 6**, in the first question to use the common use cases, respondent input confirms that their "commercial launch" priorities are strongly tied to NGC and NR adoption. Of these the top three areas of focus are core network signaling (47%), cloud RAN fronthaul and backhaul (44%), and core network services (35%). Services based on MEC and IoT, while still important given limited deployments before 5G, scored in the 20% to 28% range in the context of launch priority.

The lowest ranking use case – API exposure with third parties use case (19%) – confirms that this capability represents a lower initial launch priority. However, it should also be noted this use case attained the highest priority score (48%) in the "1 to 2 years after commercial launch" category, confirming it is strategically important.

Figure 6: Implementing 5G Security Use Cases



Question: When do you expect to support the following 5G security capabilities? (N=99-102)

Source: Heavy Reading

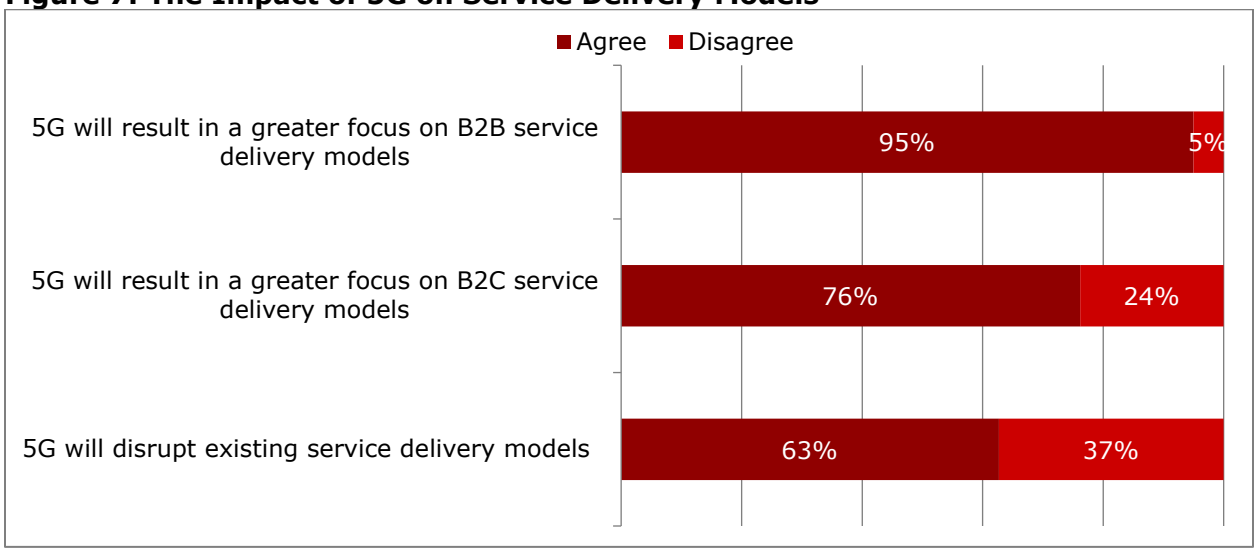
4. 5G SECURITY INVESTMENT AND MONETIZATION STRATEGIES

4.1 Slicing Up Service Delivery Models

5G is often positioned as a service delivery model disruptor, in part because of the focus on edge deployments. This is confirmed in **Figure 7**, with 63% of the survey respondents agreeing that service delivery model disruption is a reality.

As captured in the figure, it is not all bad news, because there are business opportunities to focus on both in the B2C (76%) consumer market and even greater potential in the sale of services directly to businesses (B2B – 95%). IoT services, including security-related services, are expected to figure prominently in the mix in both markets.

Figure 7: The Impact of 5G on Service Delivery Models

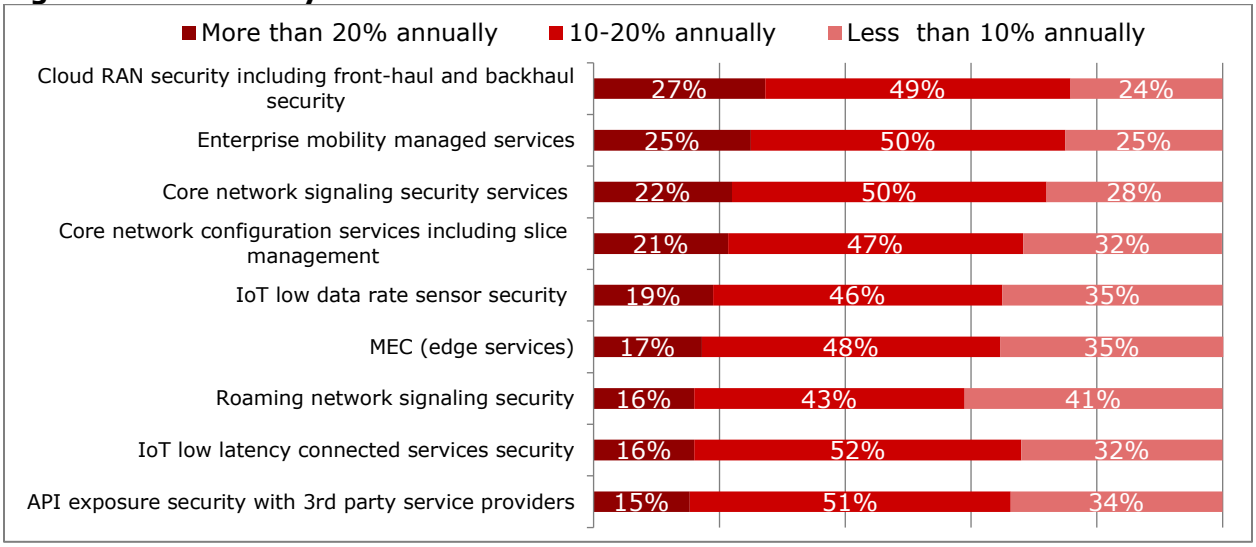


Question: Do you agree or disagree with the following statements? (N=101-102)
Source: Heavy Reading

As captured above in **Figure 6**, CSPs have chosen to start with the basics: core and RAN strategies for commercial launch. One of the key drivers for concentrating on this, as shown in **Figure 8** below, is that after 3 to 5 years, they expect cloud RAN security to be the greatest revenue generator (27%) based on "more than 20% annually" growth responses. Core security services and core network configuration services attained third- and fourth-place scoring (22% and 21%) in this same growth category.

The second-place ranking of enterprise mobility security services (25%) among the top annual growth service earners reinforces just how strategically important the delivery of cloud-based enterprise mobility managed security services has become in a relatively short period of time.

Figure 8: 5G Security Use Case Revenue Potential



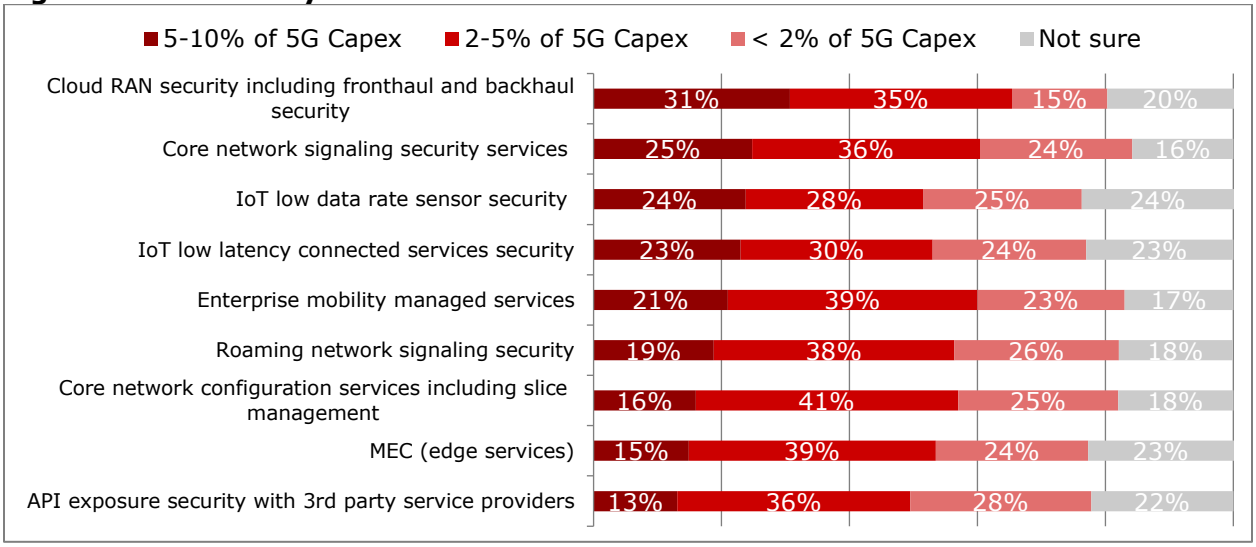
Question: Please rank the revenue potential of each use case 3 to 5 years after 5G commercial deployment. (N=98-100)
Source: Heavy Reading

Comparing the revenue potential of **Figure 8** to secure use case investment priorities in **Figure 9** below confirms that CSPs have linked investment with revenue potential at least for the top two priorities. This translates into cloud RAN security standing out as the top investment priority (31%), followed by core network signaling security services (25%).

Beyond the top two rankings, things are a little less clear. For example, IoT security services (both low data rate and low latency connected services) attained third- and fourth-place scoring metrics (24% and 23%) even though both were not viewed as high revenue generators even 3 to 5 years out in the previous figure.

The logical conclusion here is that the strategic nature of these services is so compelling in a world of changing business models that they cannot be ignored as future revenue enablers. It is also worth noting that a significant range of respondents (16% to 24%) are still unsure of their investment priorities, suggesting CAPEX allocation for 5G security services is still relatively fluid.

Figure 9: 5G Security Use Case Investment Priorities

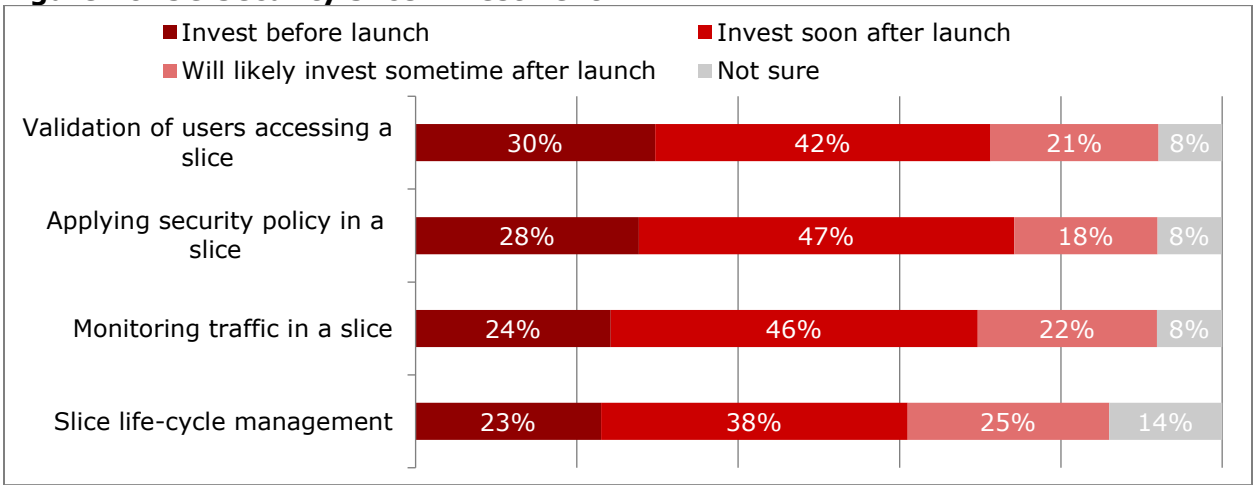


Question: How much will you invest in the following use cases 3 to 5 years after 5G commercial deployment? (N= 99-101)
Source: Heavy Reading

Support of service-specific 5G slicing is frequently presented as the network capability that is essential for achieving the true measure of 5G service innovation. However, there is a clear security cost, given that slicing security enforcement has never been commercially supported before 5G. Moreover, it is necessary to deploy the NGC to fully realize the value of slicing.

This factor is likely one reason why, as shown in **Figure 10**, less than a third of respondents (23% to 30%) actually plan to invest in specific slice security capabilities before launch is confirmed. In contrast, the top two security use cases in terms of revenue growth potential, cloud RAN and enterprise security services, can be implemented on some level without full NGC network slice support (see **Figure 8**).

Figure 10: 5G Security Slice Investment

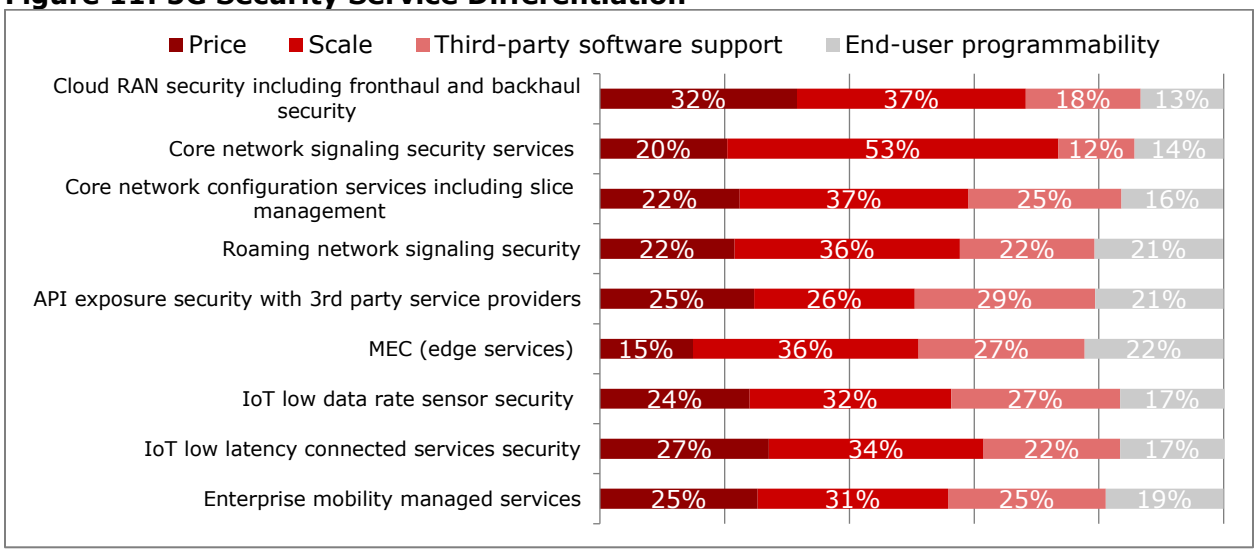


Question: When will you invest in the following 5G slice security capabilities? (N=98-101)
Source: Heavy Reading

In an environment where even vendors and OTT providers are pushing the envelope on how to monetize the 5G-fueled cloud, the challenge for CSPs is how to differentiate their security services. In response, as shown in **Figure 11**, even though each of the 5G security use cases captured below has unique requirements, the range of score metrics indicates the focus is on scale versus pricing differentiation, and then third-party software support and end-user programmability.

But to be clear, all four of these metrics are important on a use case-specific basis. For example, survey respondents ranked third-party software support as the number one consideration (29%) over price (25%) and scale (26%) for API exposure security services.

Figure 11: 5G Security Service Differentiation



Question: How will you competitively differentiate the following 5G security services? (N=94-98)
Source: Heavy Reading

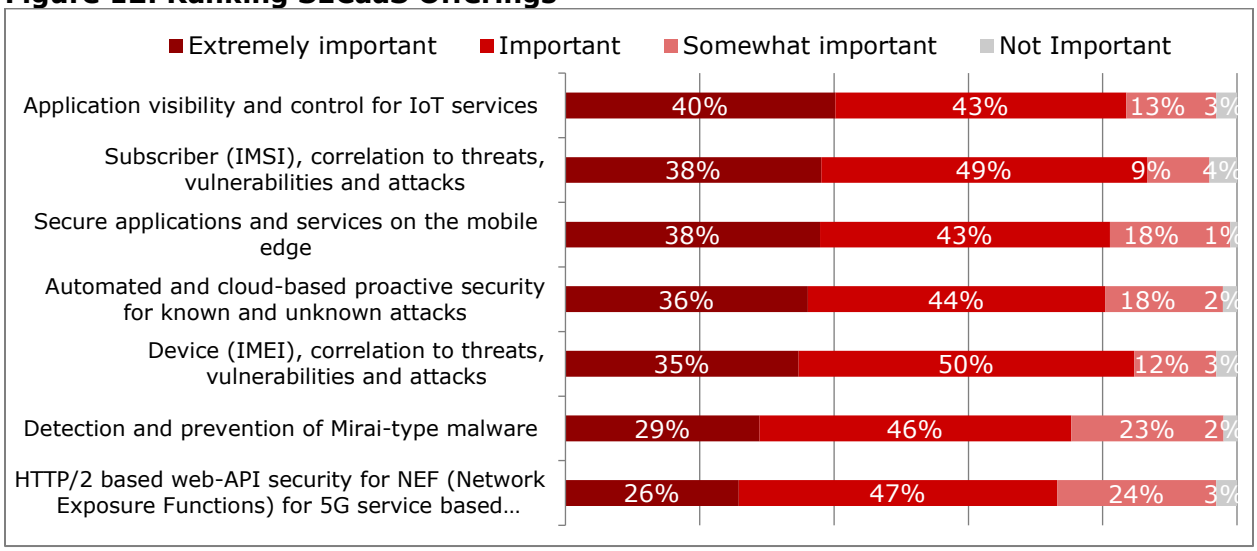
As depicted in the previous figure, CSPs are focusing on leveraging scale to differentiate 5G security services. SECaaS as a cloud-based, security-based subscription service is an excellent example of how scale can be used to achieve ubiquitous reach for the delivery of advanced software-based security features. But understanding SECaaS offerings on a granular basis is necessary in order to assess long-term market potential.

Based on the close ranking of "extremely important" responses captured in **Figure 12**, it is readily apparent that CSPs consider a number of key functions as vital to enhancing security offerings. At the top of the list is application visibility for IoT services (40%), followed closely by IMSI correlation and secure applications on the mobile edge (both 38%), then automated cloud security (36%) and IMEI threat correlation (35%).

While HTTP/2 API security for NEF-based architecture attained the lowest score of 26%, this capability should not be discounted, as it is important in terms of overall control plane security (see **Figure 18**). Therefore, a key takeaway here is that the survey respondents

understand that successful SECaaS delivery must be bolstered by a number of key and powerful security capabilities.

Figure 12: Ranking SECaaS Offerings



Question: How important are the following 5G SECaaS offerings? (N=95-98)
Source: Heavy Reading

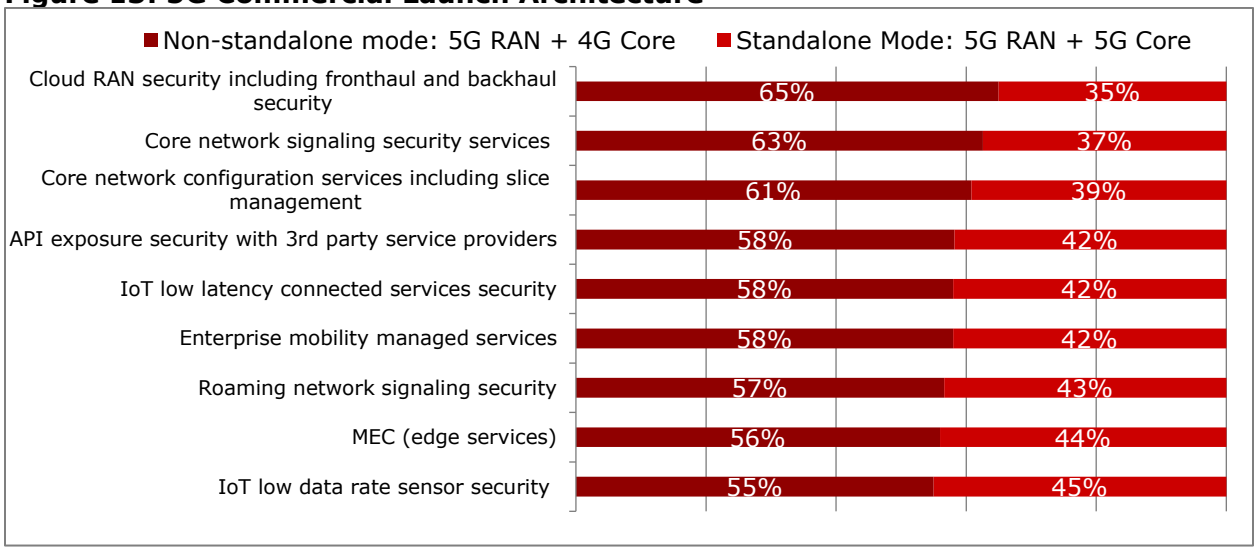
5. IMPLEMENTING THE 5G SECURITY ARCHITECTURE

5G networks can be launched using two configurations. NSA pairs the 5G NR RAN with an existing 4G core, while the SA mode implements both the 5G NR and the 5G NGC. While the SA option is positioned as the "end game" because it facilitates advanced capabilities and use cases, including slice-based use cases, it also adds more security complexity to service launch.

Therefore, understanding CSP preferences is important in order to fully understand security implications. The results shown in **Figure 13** confirm that a majority of CSPs (55% to 65%) plan to launch the common set of security use cases using the NSA option. While this does simplify security, it limits the security service reach of a number of these services.

This is one factor why Heavy Reading believes there is such a strong focus on cloud RAN security (65%) and core network signaling capabilities (63%), which must be supported in any configuration. A secondary consideration is that it also simplifies and pushes out the requirement to support 5G roaming on Internetwork Packet Exchange (IPX) networks if the original core is used for launch. Adoption of NSA also translates into less initial complexity for evolving enterprise-managed security services.

Figure 13: 5G Commercial Launch Architecture



Question: Which architecture configuration will you utilize to support the commercial launch of the following 5G security use cases? (N=97-101)
Source: Heavy Reading

As a distributed cloud-based architecture with newly defined interfaces, 5G will need to support traffic encryption on some level. Therefore, understanding encryption preferences in various layers of the network is important to understand the end-to-end security implications. Focusing on the RAN, core, and the edge, **Figure 14** captures that in the radio network, the preferred approach is to implement IPSec (54%) protocol-based encryption.

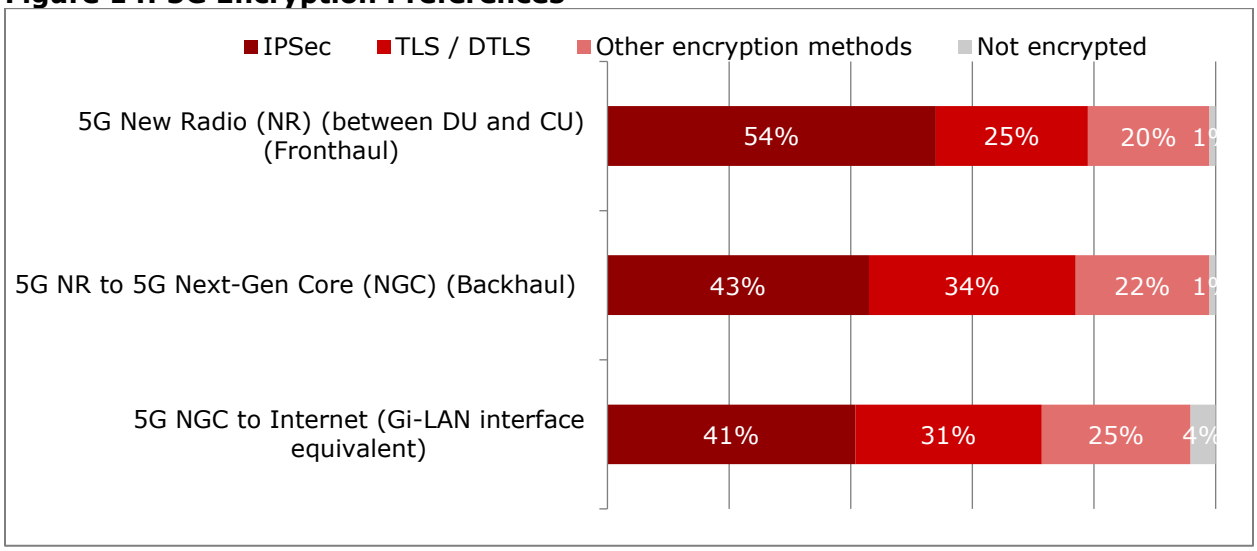
The other two layers of the networks, specifically the core and the edge/internet interface, also preferred IPSec, but with lower levels of support (43% and 41%).

The second preference to secure these network areas is to use the TLS protocol-based approach (including supporting the TLS-based DTLS option). These options, as captured in the figure, garnered solid support metrics ranging from 25% in the RAN to 34% facing the core (backhaul interfaces) and 31% core facing the internet.

Somewhat surprisingly and higher than Heavy Reading expected was the level of support of the "other" encryption methods, which fell into the 20% range in the RAN to a high of 25% for core internet-facing interface. These inputs were likely influenced by ongoing discussions to use alternative protocol-based approaches, including the Quick UDP Internet Connection (QUIC) protocol developed by Google that is optimized to manage HTTP2 services in a low latency environment.

Also of note was the fact that IPSec had generally higher support among RoW respondents than their U.S. counterparts, which had slightly greater preferences for TLS/DTLS (see **Figure 37**). The positive news is that only a very small subset of respondents (4% or less) advocated not using encryption.

Figure 14: 5G Encryption Preferences



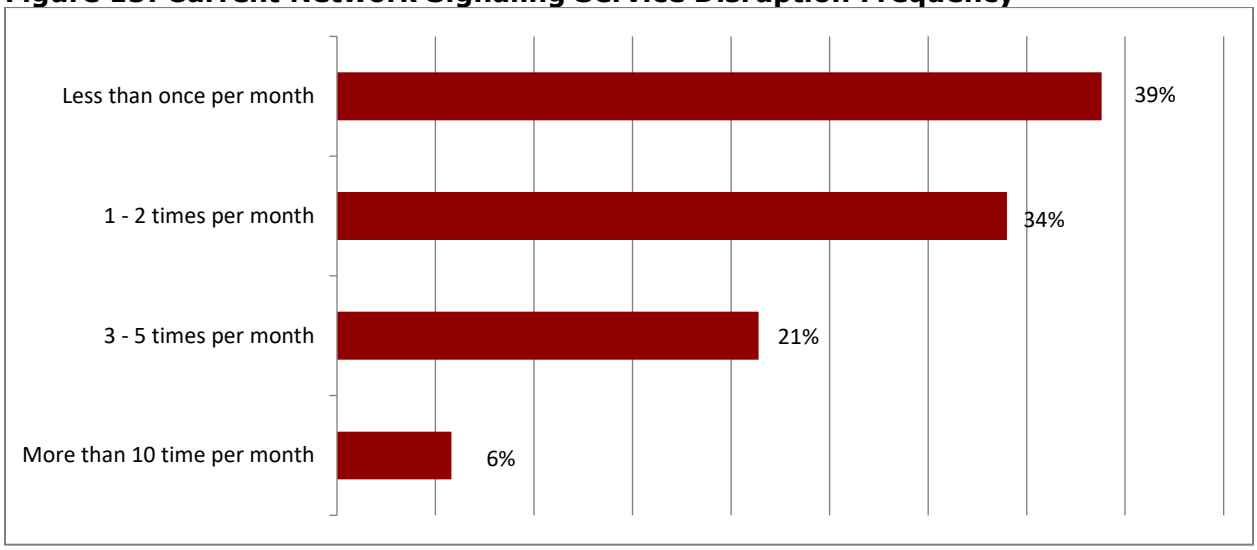
Question: What is your preferred encryption choice for securing data on the following network layers? (N=98-100)
Source: Heavy Reading

6. CONTROL PLANE CONSIDERATIONS

One of the reasons why a new 5G NGC was defined and standardized was a requirement to support more complex control plane service interactions. This applies to security policy enforcement as well. In order to understand the security implications, a number of control plane-specific questions were developed and included in the survey.

The starting point was to first benchmark the frequency of *current* network signaling service disruptions. The response levels shown in **Figure 15** confirm that CSPs are starting from a position of strength on the control plane with 39% recording essentially zero instances per month, while 34% encounter 1 to 2 service affecting instances per month. More U.S. than RoW respondents were represented in this category (see **Figure 38**).

Figure 15: Current Network Signaling Service Disruption Frequency



Question: What frequency of signaling-related service disruption (e.g., network outages) are you experiencing in your current network? (N=103)
Source: Heavy Reading

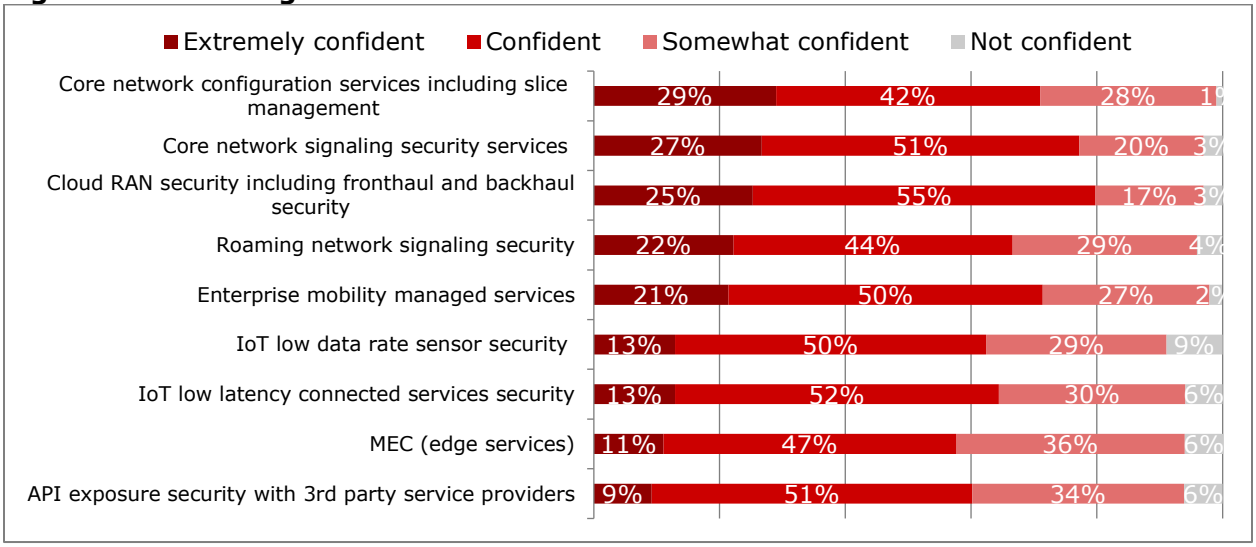
Despite encountering a very low number of outages on their existing signaling networks, survey respondents are less bullish they can achieve this same level on performance on their 5G control plane.

For instance, as shown in **Figure 16** below, typically about half of the respondents (42% to 55%) are "confident" in their abilities. While this does depict an adequate level of confidence, it is certainly not an overwhelming assertion, given the range of input on opposite ends of the spectrum. While traditional network areas, such as core network security-based services, attained the highest level of "extremely confident" responses (29% and 27%), response rates drop quickly, with IoT, MEC, and API security services falling into the 13% to 9% range.

But what is perhaps most disconcerting for these same use cases is the high rate of "somewhat confident" and "not confident" responses. When these two response rates are aggregated, it translates into a pattern in which as many as 4 out of 10 CSPs have limited

or zero confidence in their ability to secure strategically important 5G IoT-, MEC-, or API-based security use cases (see **Figures 6** and **9**).

Figure 16: Securing the 5G Control Plane

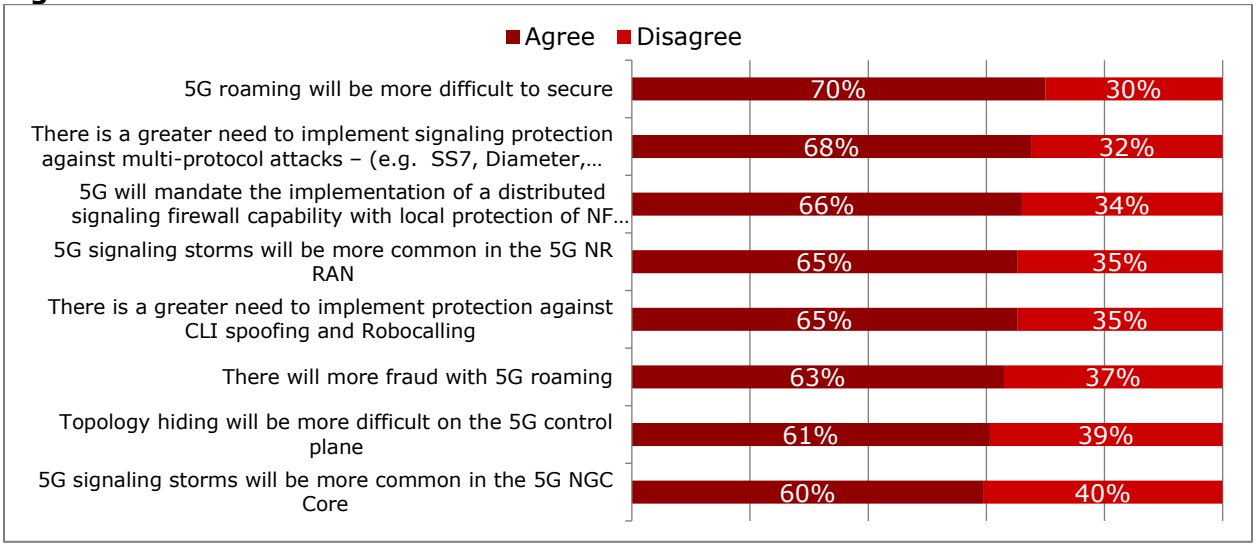


Question: How confident are you in your ability to secure the 5G control plane to support the following 5G use cases? (N=98-101)
Source: Heavy Reading

Pinpointing the exact cause(s) for why respondents are less confident in securing the 5G control plane versus current network control planes is not a simple task, but **Figure 17** provides valuable insight into their thought processes. There are several takeaways here based on the percentage of "agree" responses. The first is the high number of respondents who believe 5G roaming will be more difficult to secure (70%) and more susceptible to fraud (63%). Secondly, many respondents also believe signaling storms will be more common both in the NR and NGC (65% and 60%).

These factors also mean that security must be able to protect against multiprotocol attacks (68%), which also impacts the need to deploy distributed signaling firewalls (66%) that can play a role in managing topology hiding challenges (61%), as well as improving responses to threat vectors using CLI spoofing and robocalling (65%).

Figure 17: 5G vs. 3G and 4G Control Plane



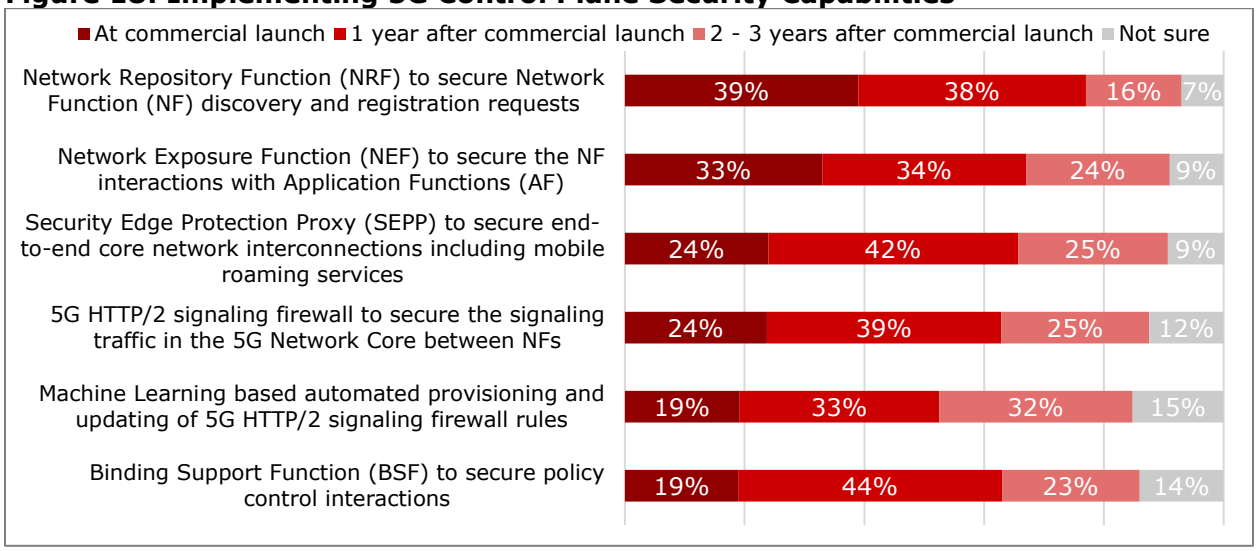
Question: Compared to 3G or 4G, please indicate whether you agree or disagree with the following statements in a 5G context. (N=97-100)
Source: Heavy Reading

Following confirmation that the 5G control plane does present new unique challenges, the next step was to investigate the timeline for supporting security-related functions, such as the SEPP and NRF to assist in risk mitigation.

The responses shown in **Figure 18** below identify that of these functions, the NRF is mostly likely to be implemented at commercial launch (39%) to enable service profile discovery, which is a key network function. The NEF, which is also service related is also seen as a commercial priority (33%). Tied for third place (24%) were the SEPP, which secures roaming at the edge, and the 5G signaling firewall, which as noted later will play a key role in signaling security.

Furthermore, while still early days, machine learning-based automated provisioning and policy enforcement attracted significant commercial launch support (19%). (See **Figure 23**.)

Figure 18: Implementing 5G Control Plane Security Capabilities



Question: When do you expect to implement the following 5G control plane security capabilities? (N=96-100)
Source: Heavy Reading

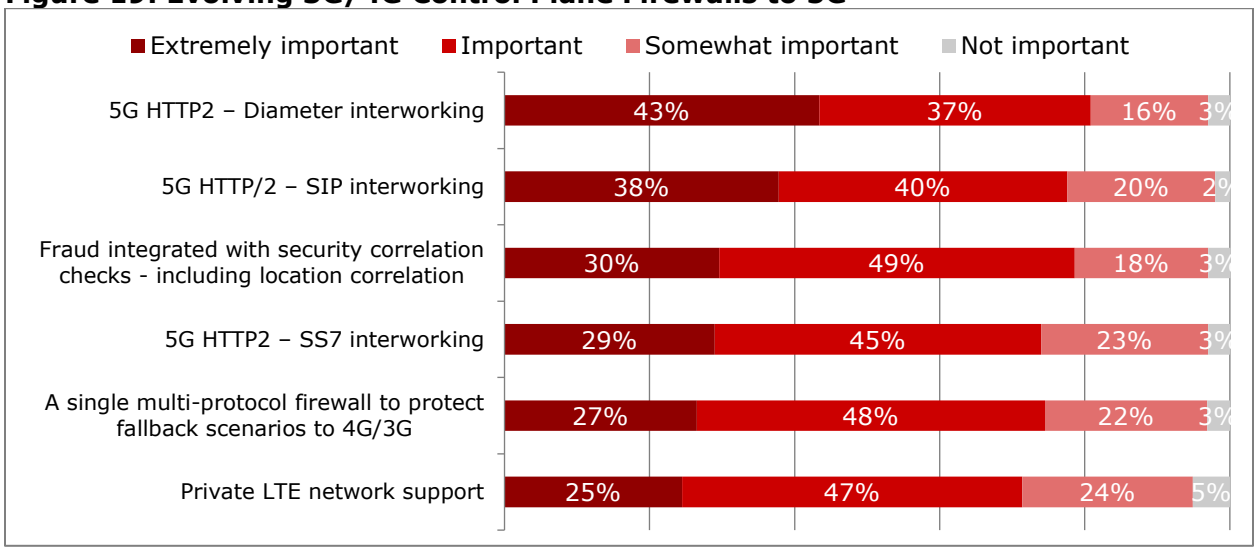
One of the challenges CSPs face with the control plane is not just managing the unique 5G security requirements in isolation, but rather managing them in a hybrid environment to ensure seamless interworking of 3G and 4G signaling protocols.

One important consideration in this process is the extent to which existing 3G and 4G control plane firewalls can evolve to support 5G. **Figure 19** below provides valuable insight into which capabilities the respondents consider most important in this journey.

While all the attributes listed in the question had significant levels of support, based on "extremely important" inputs, the respondents tended to gravitate toward HTTP2 – Diameter interworking (43%), HTTP2 – SIP interworking (38%), and then fraud/correlation capabilities (30%), HTTP2 – SS7 interworking (29%), and single/multiprotocol support firewall (27%), which reflects the need to support HTTP2 Diameter, SIP, and even SS7 interworking.

The level of "important" responses (37% to 49%) is also significant. It reaffirms the focus on fraud/correlation (49%), single multiprotocol firewall (48%), and even the importance of private Long-Term Evolution (LTE) network support (47%), which continues to gain market traction.

Figure 19: Evolving 3G/4G Control Plane Firewalls to 5G

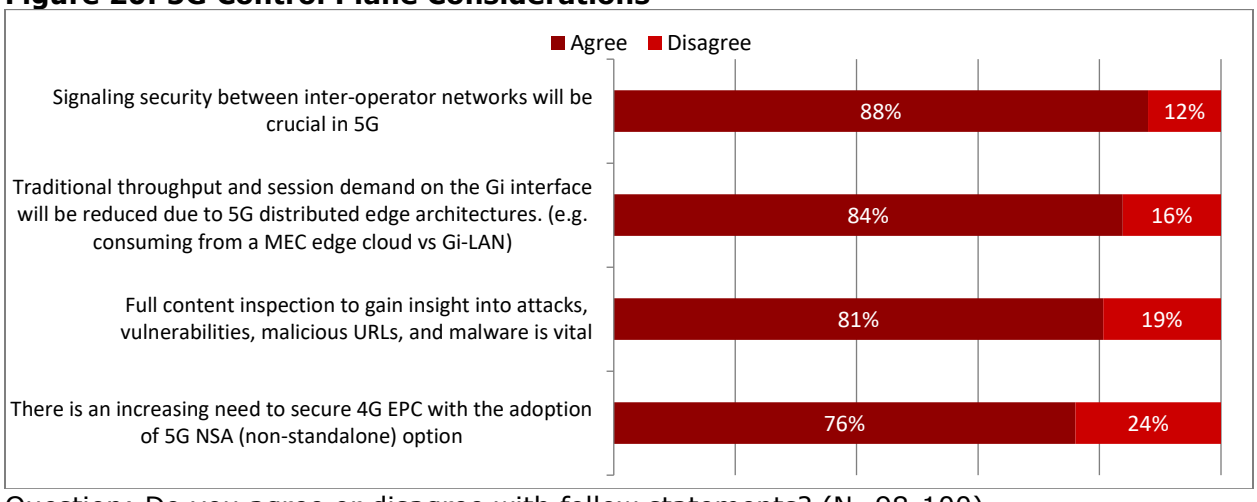


Question: How important is it for your existing 3G/4G control plane firewall to support the following 5G capabilities at 5G commercial launch? (N=98-100)
Source: Heavy Reading

The final control plane-related survey question was designed to provide insight into the relative value of additional control plane security-related capabilities.

The range of "agree" response data (88% to 76%) shown in **Figure 20** confirms there is little disagreement that advanced signaling security requirements will be necessary. The key takeaways here are that signaling security between inter-operator networks is crucial (88%), that the implementation of a 5G distributed architecture will drive a reduction of traffic on existing interfaces such as Gi-LAN (84%), that content inspection is vital (81%) to provide insight into attacks, and that when the NSA option is implemented, there is a requirement to upgrade the security capabilities of the existing Evolved Packet Core (EPC) (76%).

Figure 20: 5G Control Plane Considerations



Question: Do you agree or disagree with follow statements? (N=98-100)
Source: Heavy Reading

7. THREAT AND FRAUD MITIGATION

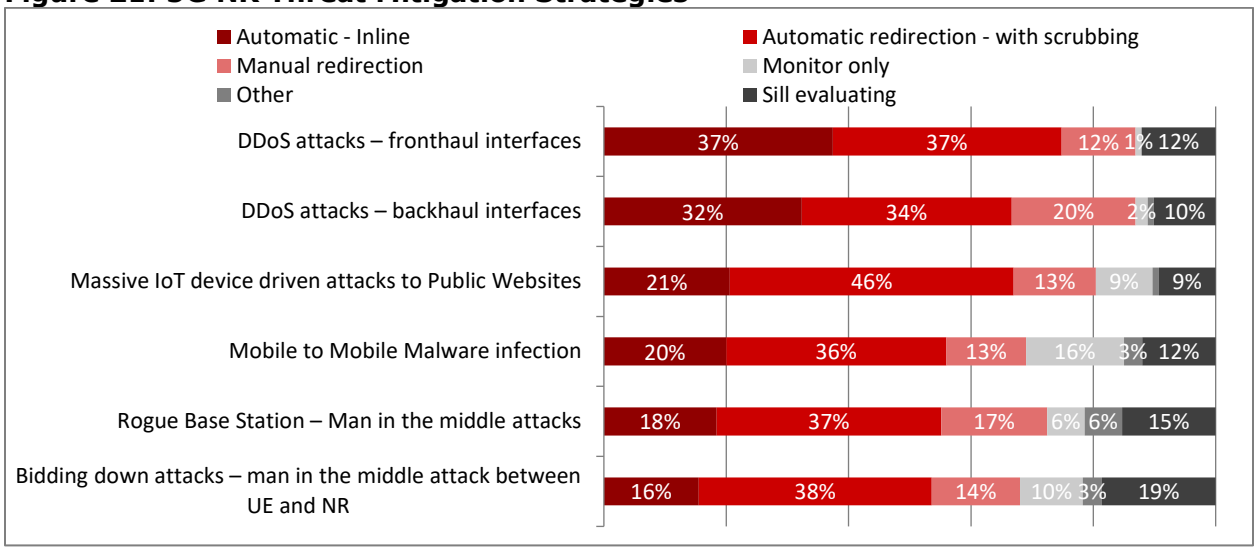
7.1 Evading the Long Shadow

A number of the figures from the previous section highlight an underlying level of concern that CSPs have with respect to managing 5G-specific fraud and threat vectors. Therefore, putting in place effective threat and fraud mitigation strategies is vital to ensuring that 5G commercial success is not negatively impacted by the long shadow that security breaches and fraud events cast upon the marketplace.

5G NR is no exception, because it represents a new threat and fraud target. There are a number of approaches that can be taken depending on the type of threat confronted, but as **Figure 21** shows, generally the respondents (34% to 46%) gravitate toward using automatic threat redirection to send malicious traffic to a scrubbing center. The greatest level of support for this approach was to manage IoT attacks from public websites (46%), while distributed denial-of-service (DDoS) attacks on backhaul interfaces attained the lowest score (34%).

The response data also shows that many respondents are split on which other alternative to use. The second camp, which attained higher scores on the top end, favored the more comprehensive automatic, inline scanning approach (16% to 37%), with the greatest support noted for managing DDoS attacks on both fronthaul (37%) and backhaul (32%) interfaces. The third group advocated support of the more basic manual redirection approach (12% to 20%).

Figure 21: 5G NR Threat Mitigation Strategies



Question: Which approach will you utilize to mitigate the impact of the following threat types targeting 5G NR? (N=97-100)
Source: Heavy Reading

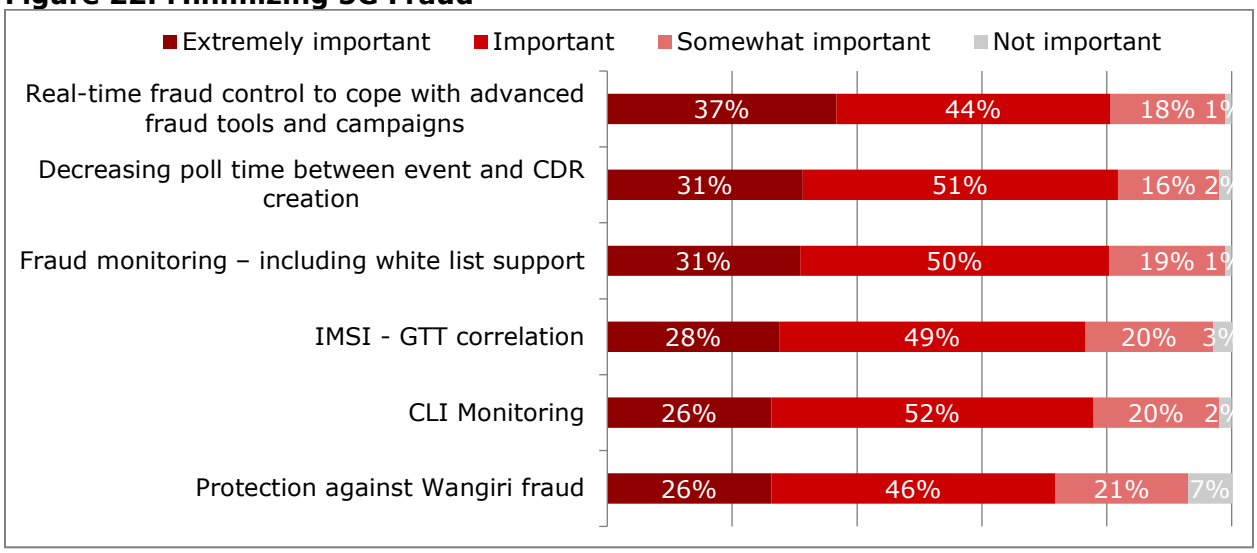
As illustrated in **Figure 19**, a number of security capabilities, including those supported by firewalls, must be implemented to minimize fraud. **Figure 22** below provides additional insight into the various capabilities that CSPs will deploy to address fraud-related challenges. In looking at the range of "extremely important" responses, the first thing that

stands out is that all the capabilities listed in the figure are viewed as extremely important. While real-time fraud tools lead the pack at 37%, the others are not far behind.

This is significant because these capabilities are unique and broad in scope. They address optimization of the alignment of billing functions, such as polling and CDR creation (31%), enhancing white list support (31%), control plane correlation between the IMSI, which identifies the subscriber, and GTT, which is used to route signaling messages (28%).

Also of importance is the ability to monitor the CLI of numbers initiating calls (26%) and even specific tools to mitigate the overbilling impact of Wangiri fraud (26%).

Figure 22: Minimizing 5G Fraud



Question: How important are the following capabilities toward minimizing 5G fraud? (N=97-99)
Source: Heavy Reading

8. AUTOMATION AND OTHER ADVANCED CAPABILITIES

8.1 Automation as a Logical Starting Point

As 5G networks mature and evolve, automation capabilities, including automated security policy and other advanced capabilities such as content inspection, will play an increasing role in security.

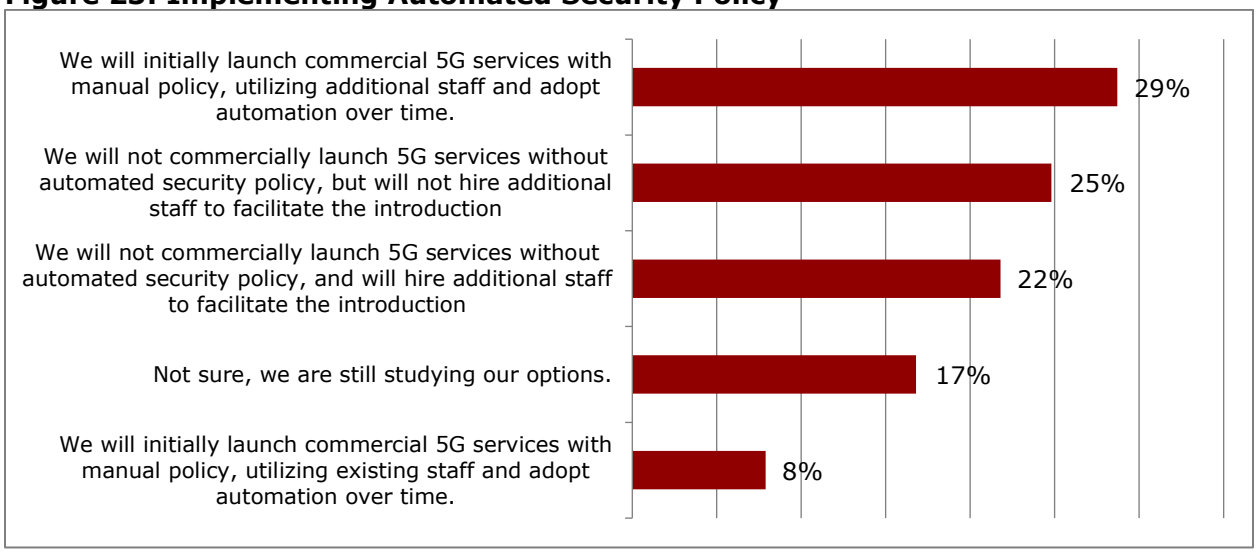
Automation is a logical starting point, because it provides the necessary technology base on which to build. Accordingly, the survey first investigated the pace of implementing automated security policy, as well as the staffing implications. The top three data inputs shown in **Figure 23** captured support for a number of approaches.

The most common sentiment among the respondents by a slight margin was that CSPs would launch commercial 5G services using manual policy and adopt automation over time (29%).

In contrast, the second group, would not launch 5G without an automated security policy, but would not hire additional staff (25%). The third group was very similar to the second, except these respondents would hire additional staff to facilitate the rollout (22%). Based on second and third response rates, almost half of the respondents (25%+22% = 47%) appear committed to implementing automated security policy. At the other end of the spectrum, only 8% of respondents adopted the "status quo" approach of using a manual policy with existing staff.

Considerable differences in the response trends between U.S. and RoW respondents were noted here. While 38% of U.S. respondents planned to implement the first approach (manual policy – automation over time – additional staff), only 20% of RoW respondents advocate this approach (see **Figure 46**).

Figure 23: Implementing Automated Security Policy



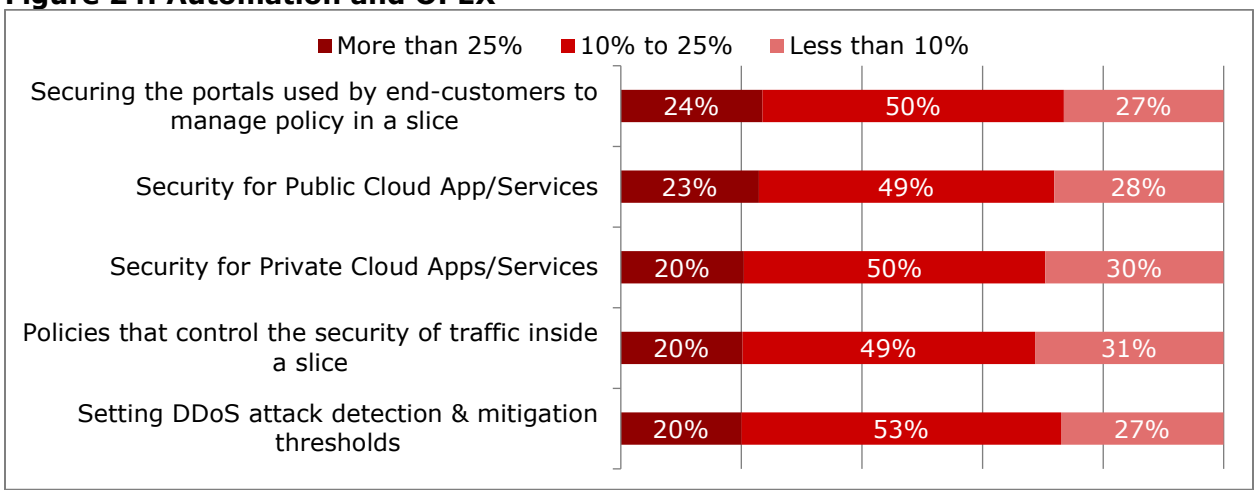
Question: Which statement best reflects your automated security policy adoption strategy when deploying 5G networks? (N=101)
Source: Heavy Reading

In addition to enhancing security policy performance, automation is often positioned as driving a meaningful reduction in OPEX associated with securing 5G networks. Survey responses captured in **Figure 24** reinforce this sentiment.

For instance, essentially half the respondents (49% to 53%) believe that automated policy will reduce OPEX at a level of 10% to 25% for all the use cases listed, including DDoS attack detection (53%), security for both public and private cloud applications and services (49% and 50%), and slice-related security (end-customer portal, 50%, and traffic security in a slice, 49%).

At the other end are two groups. The slightly larger group (27% to 31%) adopts the most pragmatic approach and gauges OPEX savings in the less than 10% range, while the third most aggressive group (20% to 24%) forecasts an OPEX reduction of more than 25%. Combining the two upper scoring groups results in about 70% of respondents forecasting at least a 10% OPEX reduction.

Figure 24: Automation and OPEX



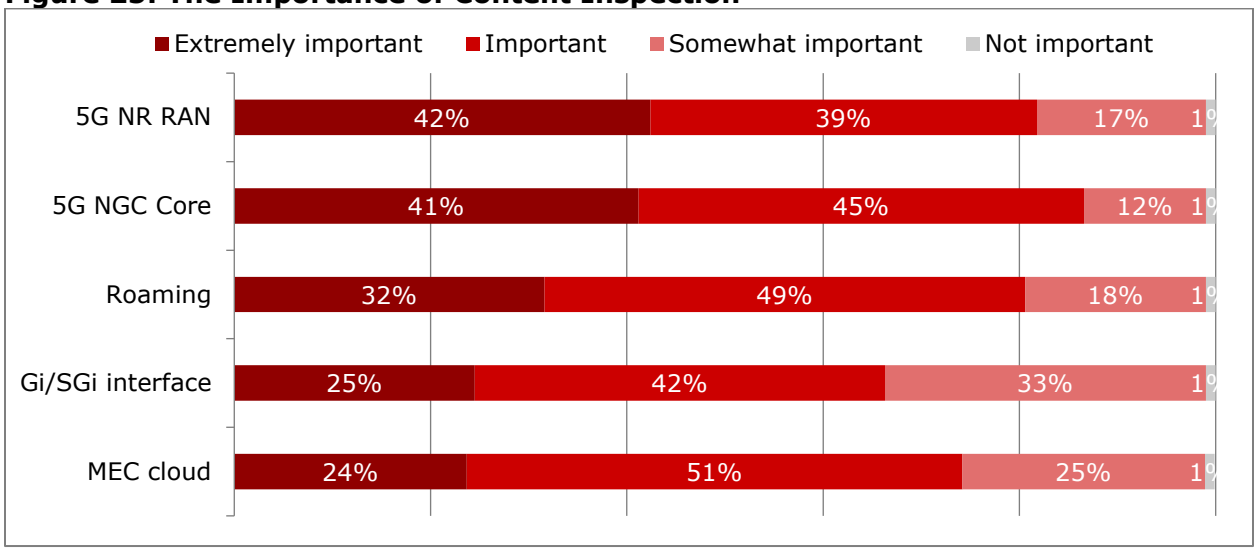
Question: What is the OPEX reduction potential for the following automated 5G security policy focus areas? (N=96-100)
Source: Heavy Reading

The value of content inspection to provide insight into attacks was first noted in **Figure 20**. However, **Figure 25** below serves to close the feedback loop, especially with the RAN and core where 42% and 41% of respondents are evaluating content inspection as "extremely important."

The percentage of "extremely important" response levels drops off for roaming (32%), implementing on the Gi-LAN (25%), and MEC (24%) responses. However, the strong

proportion of "important" responses for these three (49%, 42%, and 51%, respectively) validates that content inspection is a valuable threat mitigation tool.

Figure 25: The Importance of Content Inspection



Question: How important is the application of full content inspection to gain insight into attacks, vulnerabilities, malicious URLs, and malware? (N=97-99)
Source: Heavy Reading

9. SELECTING 5G SECURITY VENDORS

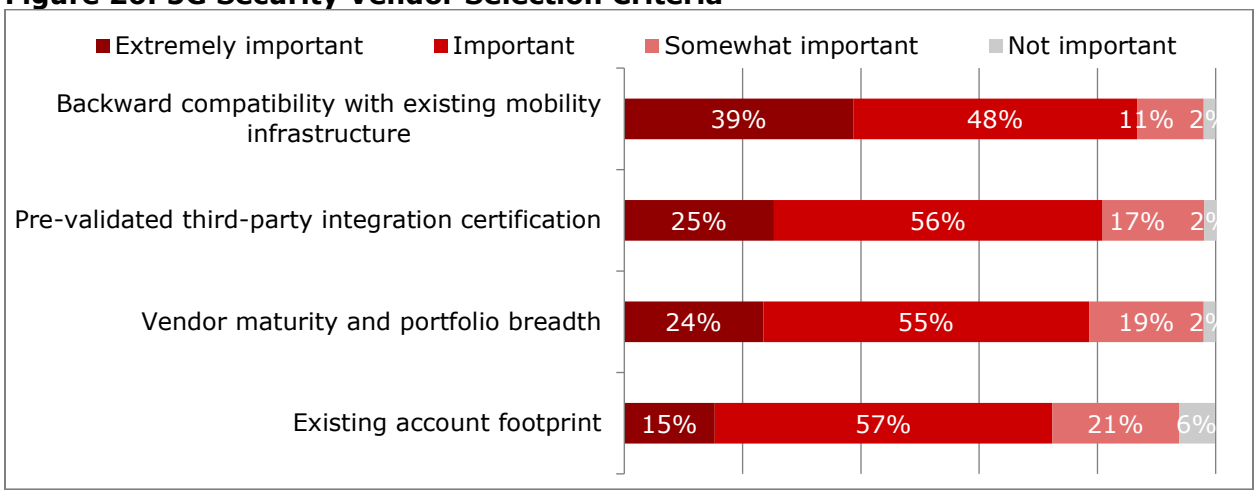
In the final section of the survey, respondents were asked to share their views on the attributes considered when selecting 5G security vendors and signaling security and fraud specialists.

9.1 Backward Compatibility, Third-Party Certification, and Programmability Are Key

As **Figure 26** shows, when respondents select security vendors, the three factors they consider as "extremely important" are backward compatibility (39%), third-party integration certification (25%), and portfolio breadth and maturity (24%). Interestingly, existing vendor footprint was last on the list (15%), which suggests that CSPs are open to working with new vendors if they meet the top three criteria.

Although existing footprint vendors will undoubtedly attempt to sway CSPs to believe that only an incumbent vendor can meet the criteria, it does point to opportunities for progressive security vendors to gain greater account penetration, because service providers typically already have a number of security vendors in their network and 5G is seen as an opportunity to consolidate the number with the implementation of a common distributed architecture.

Figure 26: 5G Security Vendor Selection Criteria

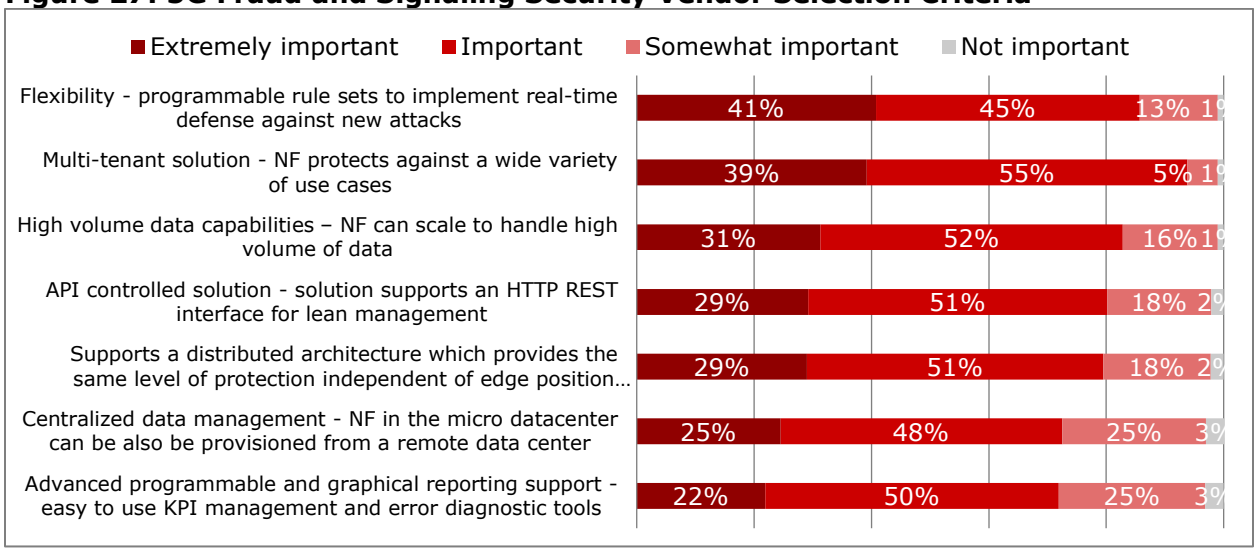


Question: How important are the following factors when selecting 5G security vendors? (N=98-99)
Source: Heavy Reading

Extending the selection discussion to signaling and fraud-specific vendors using more granular criteria, two attributes stand out. As shown in **Figure 27**, based on "extremely important" responses, these are programmable rule sets (41%) and multi-tenant use case support (39%), with other attributes, such as scale (31%), API/REST support (29%), and distributed architecture design (29%) still achieving solid support levels.

The message from this input is clear: signaling and fraud solutions must be programmable and scalable, multi-tenanted, and API-controllable to meet the real-time needs of distributed architecture configurations.

Figure 27: 5G Fraud and Signaling Security Vendor Selection Criteria



Question: How important are the following network function (NF) capabilities when selecting a 5G control plane vendor to support 5G and MEC signaling security and fraud protection? (N=93-99)

Source: Heavy Reading

10. APPENDIX A: FILTER GROUP DATA

This appendix provides question response data for the two filter groups: the U.S. and the RoW. Key findings addressing response similarity and differences are also provided.

Figure 28: 5G Security Capability Trial Priorities: U.S. vs. RoW
U.S. (N=49)

NB-IoT security including RAN monitoring	44%
Edge cloud security	58%
Per-slice security	50%
Signaling security on roaming GRX/IPX networks	27%

RoW (N=54)

NB-IoT security including RAN monitoring	72%
Edge cloud security	56%
Per-slice security	32%
Signaling security on roaming GRX/IPX networks	37%

Question: Which security capabilities will you focus on during 5G pilot trails (select all that apply)?
Source: Heavy Reading

Key Findings

While U.S. and RoW respondents are aligned on the priority ranking of edge cloud security as a trial priority (58% and 56%, respectively), RoW respondents have a much greater trial focus on NB-IoT than U.S. respondents (72% vs. 44%), while the inverse is true for per-slice security. In this case, U.S. respondents have a stronger trial focus of per-slice security than RoW respondents (50% vs. 32%). (See **Figures 33** and **36**.) Additionally, RoW respondents are more focused on signaling security for roaming than their U.S. counterparts (37% vs. 27%).

Figure 29: Implementing 5G Security Use Cases: U.S. vs. RoW
U.S. (N=47-49)

	At commercial launch	1 - 2 years after commercial launch	3 - 5 years after commercial launch	Not sure
Core network signaling security services	42%	38%	15%	6%
Cloud RAN security including fronthaul and backhaul security	38%	42%	10%	10%
Core network configuration services including slice management	34%	40%	17%	9%
IoT low latency connected services security	23%	38%	27%	13%
Enterprise mobility managed services	23%	45%	19%	13%
IoT low data rate sensor security	15%	50%	23%	13%
Roaming network signaling security	19%	54%	21%	6%
MEC (edge services)	25%	40%	21%	15%
API exposure security with 3rd party service providers	15%	56%	19%	10%

RoW (N=51-54)

	At commercial launch	1 - 2 years after commercial launch	3 - 5 years after commercial launch	Not sure
Core network signaling security services	51%	30%	13%	6%
Cloud RAN security including fronthaul and backhaul security	50%	33%	7%	9%
Core network configuration services including slice management	37%	35%	15%	14%
IoT low latency connected services security	33%	41%	13%	13%
Enterprise mobility managed services	30%	36%	17%	17%
IoT low data rate sensor security	37%	43%	15%	6%
Roaming network signaling security	33%	37%	18%	12%
MEC (edge services)	15%	45%	23%	17%
API exposure security with 3rd party service providers	23%	40%	25%	12%

Question: When do you expect to support the following 5G security capabilities?
Source: Heavy Reading

Key Findings

While data trends are similar, RoW respondents are slightly more committed to implementing capabilities such as signaling security services (51% vs. 42%) and cloud RAN security services (50% vs. 38%) at commercial launch.

Figure 30: The Impact of 5G on Service Delivery Models: U.S. vs. RoW
U.S. (N=47-48)

	Agree	Disagree
5G will result in a greater focus on B2B service delivery models	100%	0%
5G will result in a greater focus on B2C service delivery models	85%	15%
5G will disrupt existing service delivery models	65%	35%

RoW (N=54)

	Agree	Disagree
5G will result in a greater focus on B2B service delivery models	91%	9%
5G will result in a greater focus on B2C service delivery models	69%	32%
5G will disrupt existing service delivery models	61%	39%

Question: Do you agree or disagree with the following statements?
Source: Heavy Reading

Key Findings

There is a strong level of agreement here on the impact of 5G on service delivery models. U.S. respondents are, however, anticipating an even greater focus on B2C service delivery than RoW respondents (85% vs. 69%), perhaps because of the initial focus on using 5G in the U.S. for fixed mobility residential broadband services.

Figure 31: 5G Security Use Case Revenue Potential: U.S. vs. RoW

U.S. (N=46-47)

	More than 20% annually	10-20% annually	Less than 10% annually
Cloud RAN security including front-haul and backhaul security	28%	51%	21%
Enterprise mobility managed services	24%	50%	26%
Core network signaling security services	26%	53%	21%
Core network configuration services including slice management	20%	52%	28%
IoT low data rate sensor security	15%	46%	39%
MEC (edge services)	20%	50%	30%
Roaming network signaling security	11%	52%	37%
IoT low latency connected services security	9%	54%	37%
API exposure security with 3rd party service providers	20%	50%	30%

RoW (N=52-54)

	More than 20% annually	10-20% annually	Less than 10% annually
Cloud RAN security including front-haul and backhaul security	27%	46%	27%
Enterprise mobility managed services	26%	50%	24%
Core network signaling security services	19%	47%	34%
Core network configuration services including slice management	23%	42%	35%
IoT low data rate sensor security	22%	46%	32%
MEC (edge services)	15%	45%	40%
Roaming network signaling security	20%	35%	44%
IoT low latency connected services security	22%	50%	28%
API exposure security with 3rd party service providers	12%	52%	37%

Question: Please rank the revenue potential of each use case 3 to 5 years after 5G commercial deployment.

Source: Heavy Reading

Key Findings

Both groups share similar views on the long-term revenue potential of security services based on use case rankings. Of note is the fact that RoW respondents view IoT low latency security services as a greater revenue opportunity, with 22% assessing as achieving more than 20% annual growth compared to 9% of U.S. respondents.

Figure 32: 5G Security Use Case Investment Priorities: U.S. vs. RoW

U.S. (N=46-48)

	5-10% of 5G Capex	2-5% of 5G Capex	< 2% of 5G Capex	Not sure
Cloud RAN security including fronthaul and backhaul security	33%	29%	15%	23%
Core network signaling security services	27%	33%	23%	17%
IoT low data rate sensor security	21%	32%	26%	21%
IoT low latency connected services security	19%	34%	26%	21%
Enterprise mobility managed services	26%	37%	22%	15%
Roaming network signaling security	19%	47%	19%	15%
Core network configuration services including slice management	21%	36%	26%	17%
MEC (edge services)	19%	36%	30%	15%
API exposure security with 3rd party service providers	13%	38%	28%	21%

RoW (N=52-54)

	5-10% of 5G Capex	2-5% of 5G Capex	< 2% of 5G Capex	Not sure
Cloud RAN security including fronthaul and backhaul security	28%	40%	15%	17%
Core network signaling security services	23%	38%	25%	15%
IoT low data rate sensor security	26%	24%	24%	26%
IoT low latency connected services security	26%	26%	23%	25%
Enterprise mobility managed services	17%	41%	24%	19%
Roaming network signaling security	19%	30%	32%	20%
Core network configuration services including slice management	11%	45%	25%	19%
MEC (edge services)	11%	41%	19%	30%
API exposure security with 3rd party service providers	14%	35%	29%	23%

Question: How much will you invest in the following use cases 3-5 years after 5G commercial deployment?
Source: Heavy Reading

Key Findings

While there is a general level of consensus on CAPEX commitment, U.S. respondents forecast slightly greater demand for investment on the higher end (5% to 10% of CAPEX) than RoW respondents (13% to 33% vs. 11% to 28%, respectively). One consideration may be the greater commitment of U.S. respondents to the SA architecture, which increases CAPEX spending (see **Figure 36**), especially in the core, where U.S. respondents anticipate the greatest level of investment (21% vs. 11%).

Figure 33: 5G Security Slice Investment: U.S. vs. RoW
U.S. (N=47)

	Invest before launch	Invest soon after launch	Will likely invest sometime after launch	Not sure
Validation of users accessing a slice	32%	38%	26%	4%
Applying security policy in a slice	23%	60%	13%	4%
Monitoring traffic in a slice	23%	53%	17%	6%
Slice life-cycle management	21%	45%	21%	13%

RoW (N=52-54)

	Invest before launch	Invest soon after launch	Will likely invest sometime after launch	Not sure
Validation of users accessing a slice	28%	44%	17%	11%
Applying security policy in a slice	32%	35%	22%	11%
Monitoring traffic in a slice	25%	39%	27%	10%
Slice life-cycle management	25%	32%	28%	15%

Question: When will you invest in the following 5G slice security capabilities?
Source: Heavy Reading

Key Findings

As noted above, U.S. respondents forecast greater core investment, but overall, both groups are fairly aligned on the limited need to invest in specific slice use cases before launch (U.S. 21% to 32% vs. RoW 25% to 32%). Also worth noting is the greater

commitment of the RoW to invest in applying security policy in a slice before launch than U.S. respondents. (RoW 32% vs. U.S. 23%).

Figure 34: 5G Security Service Differentiation: U.S. vs. RoW

U.S. (N=45-46)

	Price	Scale	Third-party software support	End-user programmability
Cloud RAN security including fronthaul and backhaul security	28%	35%	20%	17%
Core network signaling security services	20%	50%	9%	22%
Core network configuration services including slice management	17%	33%	22%	28%
Roaming network signaling security	28%	28%	24%	20%
API exposure security with 3rd party service providers	29%	27%	27%	18%
MEC (edge services)	24%	35%	17%	24%
IoT low data rate sensor security	27%	24%	31%	18%
IoT low latency connected services security	36%	27%	20%	18%
Enterprise mobility managed services	29%	29%	22%	20%

RoW (N=48-52)

	Price	Scale	Third-party software support	End-user programmability
Cloud RAN security including fronthaul and backhaul security	35%	39%	17%	10%
Core network signaling security services	21%	56%	15%	8%
Core network configuration services including slice management	27%	40%	27%	6%
Roaming network signaling security	16%	43%	20%	22%
API exposure security with 3rd party service providers	21%	25%	31%	23%
MEC (edge services)	6%	38%	35%	21%
IoT low data rate sensor security	22%	39%	24%	16%
IoT low latency connected services security	20%	41%	24%	16%
Enterprise mobility managed services	22%	32%	28%	18%

Question: How will you competitively differentiate the following 5G security services?
Source: Heavy Reading

Key Findings

Scale is generally viewed by both groups as the greatest opportunity to differentiate their 5G security services. One exception to this relates to IoT low latency connected services security versus price. While RoW respondents rank scale at 41%, U.S. respondents rank it at 27%. U.S. respondents also anticipate a greater opportunity to differentiate based on price for these services than RoW respondents (36% vs. 20%).

On some level, competitive landscape differences between the U.S. and the RoW are likely a factor influencing the relative weighting of pricing.

Figure 35: Ranking SECaaS Offerings: U.S. vs. RoW

U.S. (N=46-47)

	Extremely important	Important	Somewhat important	Not Important
Application visibility and control for IoT services	39%	50%	9%	2%
Subscriber (IMSI), correlation to threats, vulnerabilities and attacks	45%	43%	9%	4%
Secure applications and services on the mobile edge	44%	41%	15%	0%
Automated and cloud-based proactive security for known and unknown attacks	41%	39%	20%	0%
Device (IMEI), correlation to threats, vulnerabilities and attacks	38%	49%	13%	0%
Detection and prevention of Mirai-type malware	35%	46%	17%	2%
HTTP/2 based web-API security for NEF (Network Exposure Functions) for 5G service based architectures	33%	41%	26%	0%

RoW (N=49-51)

	Extremely important	Important	Somewhat important	Not Important
Application visibility and control for IoT services	41%	37%	18%	4%
Subscriber (IMSI), correlation to threats, vulnerabilities and attacks	32%	54%	10%	4%
Secure applications and services on the mobile edge	33%	45%	20%	2%
Automated and cloud-based proactive security for known and unknown attacks	31%	49%	16%	4%
Device (IMEI), correlation to threats, vulnerabilities and attacks	31%	51%	12%	6%
Detection and prevention of Mirai-type malware	24%	47%	28%	2%
HTTP/2 based web-API security for NEF (Network Exposure Functions) for 5G service based architectures	20%	53%	22%	6%

Question: How important are the following 5G SECaaS offerings?

Source: Heavy Reading

Key Findings

The range of U.S. respondents' "extremely important" response level is considerably greater than RoW respondents (U.S. 33% to 45% vs. RoW 20% to 41%), suggesting SECaaS services in the U.S. are more advanced than in other countries. This may be, in part, because of the strong demand for SECaaS in the U.S. due to its status as a desirable target for cyberattacks.

Figure 36: 5G Commercial Launch Architecture: U.S. vs. RoW

U.S. (N=45-47)

	Non-standalone mode: 5G RAN + 4G Core	Standalone Mode: 5G RAN + 5G Core
Cloud RAN security including fronthaul and backhaul security	57%	43%
Core network signaling security services	54%	46%
Core network configuration services including slice management	60%	40%
API exposure security with 3rd party service providers	59%	41%
IoT low latency connected services security	48%	52%
Enterprise mobility managed services	46%	54%
Roaming network signaling security	41%	59%
MEC (edge services)	54%	46%
IoT low data rate sensor security	41%	59%

RoW (N=52-54)

	Non-standalone mode: 5G RAN + 4G Core	Standalone Mode: 5G RAN + 5G Core
Cloud RAN security including fronthaul and backhaul security	72%	28%
Core network signaling security services	70%	30%
Core network configuration services including slice management	62%	39%
API exposure security with 3rd party service providers	58%	42%
IoT low latency connected services security	67%	33%
Enterprise mobility managed services	69%	32%
Roaming network signaling security	70%	30%
MEC (edge services)	57%	43%
IoT low data rate sensor security	67%	33%

Question: Which architecture configuration will you utilize to support the commercial launch of the following 5G security use cases?

Source: Heavy Reading

Key Findings

U.S. respondents are more committed to supporting 5G security use cases with a SA architecture (40% to 59%) versus RoW respondents whose SA responses fall into the 28% to 43% range. This input is also consistent with press releases and anecdotal evidence, which suggest there is more interest in SA by U.S. carriers than their RoW counterparts.

Figure 37: 5G Encryption Preferences: U.S. vs. RoW

U.S. (N=45-46)

	IPSec	TLS / DTLS	Other encryption methods	Not encrypted
5G New Radio (NR) (between DU and CU) (Fronthaul)	46%	30%	24%	0%
5G NR to 5G Next-Gen Core (NGC) (Backhaul)	30%	41%	28%	0%
5G NGC to Internet (Gi-LAN interface equivalent)	36%	31%	29%	4%

RoW (N=53-54)

	IPSec	TLS / DTLS	Other encryption methods	Not encrypted
5G New Radio (NR) (between DU and CU) (Fronthaul)	61%	20%	17%	2%
5G NR to 5G Next-Gen Core (NGC) (Backhaul)	54%	28%	17%	2%
5G NGC to Internet (Gi-LAN interface equivalent)	45%	30%	21%	4%

Question: What is your preferred encryption choice for securing data on the following network layers?
Source: Heavy Reading

Key Findings

IPSec encryption is the preferred choice for both groups, but more U.S. respondents were open to using TLS/DTLS for both fronthaul (U.S. 30% vs. RoW 20%) and backhaul (U.S. 41% vs. RoW 28%). *Not* implementing encryption is a non-starter for both groups.

Figure 38: Current Network Signaling Service Disruption Frequency: U.S. vs. RoW
U.S. (N=49)

Less than once per month	41%
1 - 2 times per month	39%
3 - 5 times per month	14%
More than 10 time per month	6%

RoW (N=53)

Less than once per month	37%
1 - 2 times per month	30%
3 - 5 times per month	28%
More than 10 time per month	6%

Question: What frequency of signaling-related service disruption (e.g., network outages) are you experiencing in your current network?
Source: Heavy Reading

Key Findings

Data trends are similar here, with 37% of U.S. and 41% of RoW respondents reporting essentially zero monthly outages (less than once per month). However, RoW respondents recorded a double rate of 3x to 5x per month outages (RoW 28% vs. U.S. 14%), which suggests the current signaling networks of U.S. operators are more robust than those of some RoW operators.

Figure 39: Securing the 5G Control Plane: U.S. vs. RoW

U.S. (N=44-48)

	Extremely confident	Confident	Somewhat confident	Not confident
Core network configuration services including slice management	34%	47%	17%	2%
Core network signaling security services	31%	52%	15%	2%
Cloud RAN security including fronthaul and backhaul security	30%	55%	11%	4%
Roaming network signaling security	20%	57%	22%	2%
Enterprise mobility managed services	30%	46%	21%	5%
IoT low data rate sensor security	15%	57%	23%	4%
IoT low latency connected services security	17%	53%	26%	4%
MEC (edge services)	17%	52%	28%	2%
API exposure security with 3rd party service providers	9%	61%	26%	4%

RoW (N=52-54)

	Extremely confident	Confident	Somewhat confident	Not confident
Core network configuration services including slice management	25%	38%	38%	0%
Core network signaling security services	23%	49%	25%	4%
Cloud RAN security including fronthaul and backhaul security	21%	54%	23%	2%
Roaming network signaling security	25%	34%	36%	6%
Enterprise mobility managed services	15%	54%	32%	0%
IoT low data rate sensor security	11%	43%	33%	13%
IoT low latency connected services security	9%	50%	33%	7%
MEC (edge services)	6%	42%	43%	9%
API exposure security with 3rd party service providers	10%	42%	40%	8%

Question: How confident are you in your ability to secure the 5G control plane to support the following 5G use cases?

Source: Heavy Reading

Key Findings

Confidence levels differ here significantly. Overall, U.S. respondents have a greater level of "extremely confident" responses than RoW respondents (U.S. 9% to 34% vs. RoW 6% to 25%). In contrast, more RoW respondents are only "somewhat confident" (RoW 23% to 43% vs. U.S. 11% to 28%), which is logical, given that the RoW is also encountering a greater number of control plane outages on their current networks (see **Figure 38**).

Figure 40: 5G vs. 3G and 4G Control Plane: U.S. vs. RoW

U.S. (N=47-48)

	Agree	Disagree
5G roaming will be more difficult to secure	70%	30%
There is a greater need to implement signaling protection against multi-protocol attacks – (e.g. SS7, Diameter, HTTP/2 and SIP)	67%	33%
5G will mandate the implementation of a distributed signaling firewall capability with local protection of NF service execution	66%	34%
5G signaling storms will be more common in the 5G NR RAN	58%	42%
There is a greater need to implement protection against CLI spoofing and Robocalling	80%	20%
There will more fraud with 5G roaming	54%	46%
Topology hiding will be more difficult on the 5G control plane	62%	38%
5G signaling storms will be more common in the 5G NGC Core	63%	37%

RoW (N=53-54)

	Agree	Disagree
5G roaming will be more difficult to secure	70%	30%
There is a greater need to implement signaling protection against multi-protocol attacks – (e.g. SS7, Diameter, HTTP/2 and SIP)	69%	32%
5G will mandate the implementation of a distributed signaling firewall capability with local protection of NF service execution	66%	34%
5G signaling storms will be more common in the 5G NR RAN	72%	28%
There is a greater need to implement protection against CLI spoofing and Robocalling	54%	46%
There will more fraud with 5G roaming	70%	30%
Topology hiding will be more difficult on the 5G control plane	59%	41%
5G signaling storms will be more common in the 5G NGC Core	57%	43%

Question: Compared to 3G or 4G, please indicate whether you agree or disagree with the following statements in a 5G context.
Source: Heavy Reading

Key Findings

There is a strong level of consensus that 5G will be more sensitive to signaling storms across all network layers, including the RAN, and that roaming will be more difficult to secure with greater fraud opportunities.

U.S. respondents were more adamant about the need to implement protection against CLI spoofing and robocalling (80%) compared to RoW respondents (54%), while RoW respondents were more concerned with 5G roaming fraud (70%) than U.S. respondents (54%).

Figure 41: Implementing 5G Control Plane Security Capabilities: U.S. vs. RoW
U.S. (N=45-47)

	At commercial launch	1 year after commercial launch	2 - 3 years after commercial launch	Not sure
Network Repository Function (NRF) to secure Network Function (NF) discovery and registration requests	45%	36%	15%	4%
Network Exposure Function (NEF) to secure the NF interactions with Application Functions (AF)	36%	38%	19%	6%
Security Edge Protection Proxy (SEPP) to secure end-to-end core network interconnections including mobile roaming services	24%	47%	24%	4%
5G HTTP/2 signaling firewall to secure the signaling traffic in the 5G Network Core between NFs	24%	42%	24%	9%
Machine Learning based automated provisioning and updating of 5G HTTP/2 signaling firewall rules	22%	46%	22%	11%
Binding Support Function (BSF) to secure policy control interactions	17%	61%	17%	4%

RoW (N=51-54)

	At commercial launch	1 year after commercial launch	2 - 3 years after commercial launch	Not sure
Network Repository Function (NRF) to secure Network Function (NF) discovery and registration requests	34%	40%	17%	9%
Network Exposure Function (NEF) to secure the NF interactions with Application Functions (AF)	30%	30%	28%	11%
Security Edge Protection Proxy (SEPP) to secure end-to-end core network interconnections including mobile roaming services	24%	37%	26%	14%
5G HTTP/2 signaling firewall to secure the signaling traffic in the 5G Network Core between NFs	23%	37%	25%	15%
Machine Learning based automated provisioning and updating of 5G HTTP/2 signaling firewall rules	17%	23%	42%	19%
Binding Support Function (BSF) to secure policy control interactions	20%	30%	28%	22%

Question: When do you expect to implement the following 5G control plane security capabilities?
Source: Heavy Reading

Key Findings

A greater portion of RoW respondents are unsure when they will implement specific 5G control plane security capabilities (RoW 9% to 22% vs. U.S. 4% to 11%). This may be a fallout of their lower confidence levels.

Figure 42: Evolving 3G/4G Control Plane Firewalls to 5G: U.S. vs. RoW
U.S. (N=45-46)

	Extremely important	Important	Somewhat important	Not important
5G HTTP2 – Diameter interworking	41%	41%	17%	0%
5G HTTP/2 – SIP interworking	35%	46%	17%	2%
Fraud integrated with security correlation checks - including location correlation	31%	51%	16%	2%
5G HTTP2 – SS7 interworking	24%	44%	30%	2%
A single multi-protocol firewall to protect fallback scenarios to 4G/3G	31%	44%	22%	2%
Private LTE network support	22%	44%	28%	7%

RoW (N=52-54)

	Extremely important	Important	Somewhat important	Not important
5G HTTP2 – Diameter interworking	45%	34%	15%	6%
5G HTTP/2 – SIP interworking	40%	35%	23%	2%
Fraud integrated with security correlation checks - including location correlation	28%	47%	21%	4%
5G HTTP2 – SS7 interworking	33%	46%	17%	4%
A single multi-protocol firewall to protect fallback scenarios to 4G/3G	23%	51%	23%	4%
Private LTE network support	27%	50%	19%	4%

Question: How important is it for your existing 3G/4G control plane firewall to support the following 5G capabilities at 5G commercial launch?
Source: Heavy Reading

Key Findings

Alignment of "extremely important" responses confirms that existing control plane firewalls must evolve to support important 5G interworking capabilities, such as HTTP2 interworking with Diameter, SIP, and even SS7. This is logical given that, as noted above, a significant number of CSPs plan to launch 5G using existing core networks via NSA mode.

Figure 43: 5G Control Plane Considerations: U.S. vs. RoW

U.S. (N=45-46)

	Agree	Disagree
Signaling security between inter-operator networks will be crucial in 5G	87%	13%
Traditional throughput and session demand on the Gi interface will be reduced due to 5G distributed edge architectures. (e.g. consuming from a MEC edge cloud vs Gi-LAN)	78%	22%
Full content inspection to gain insight into attacks, vulnerabilities, malicious URLs, and malware is vital	78%	22%
There is an increasing need to secure 4G EPC with the adoption of 5G NSA (non-standalone) option	85%	15%

RoW (N=53-54)

	Agree	Disagree
Signaling security between inter-operator networks will be crucial in 5G	89%	11%
Traditional throughput and session demand on the Gi interface will be reduced due to 5G distributed edge architectures. (e.g. consuming from a MEC edge cloud vs Gi-LAN)	89%	11%
Full content inspection to gain insight into attacks, vulnerabilities, malicious URLs, and malware is vital	83%	17%
There is an increasing need to secure 4G EPC with the adoption of 5G NSA (non-standalone) option	69%	32%

Question: Do you agree or disagree with follow statements?
Source: Heavy Reading

Key Findings

Similar to the previous figures, both groups are aligned that new approaches, such as content inspection, are important for gaining insight into attacks. Both also indicate that 5G will start to drive a traffic reduction on existing interfaces, such as the Gi-LAN, and that inter-operator signaling security will be central to securing 5G networks (see **Figure 48**).

Figure 44: 5G NR Threat Mitigation Strategies: U.S. vs. RoW
U.S. (N=46-47)

	Automatic - Inline	Automatic redirection - with scrubbing	Manual redirection	Monitor only	Other	Sill evaluating
DDoS attacks – fronthaul interfaces	38%	38%	13%	2%	0%	9%
DDoS attacks – backhaul interfaces	32%	36%	19%	2%	2%	9%
Massive IoT device driven attacks to Public Websites	19%	53%	11%	9%	0%	9%
Mobile to Mobile Malware infection	21%	43%	9%	11%	6%	11%
Rogue Base Station – Man in the middle attacks	22%	46%	9%	4%	7%	13%
Bidding down attacks – man in the middle attack between UE and NR	20%	46%	9%	4%	4%	17%

RoW (N=51-53)

	Automatic - Inline	Automatic redirection - with scrubbing	Manual redirection	Monitor only	Other	Sill evaluating
DDoS attacks – fronthaul interfaces	37%	37%	12%	0%	0%	15%
DDoS attacks – backhaul interfaces	33%	33%	21%	2%	0%	12%
Massive IoT device driven attacks to Public Websites	22%	40%	16%	10%	2%	10%
Mobile to Mobile Malware infection	19%	30%	17%	21%	0%	13%
Rogue Base Station – Man in the middle attacks	15%	29%	25%	8%	6%	17%
Bidding down attacks – man in the middle attack between UE and NR	12%	31%	20%	16%	2%	20%

Question: Which approach will you utilize to mitigate the impact of the following threat types targeting 5G NR?
Source: Heavy Reading

Key Findings

U.S. and RoW respondents are generally aligned on the value of the various approaches. For example, while 38%, 32%, and 19% of U.S. respondents preferred automatic inline monitoring for DDoS scenarios and IoT attacks, 37%, 33%, and 22% of RoW respondents did as well. Similar patterns were noted for these same three use cases with the automatic redirection option. In this case, U.S. respondent inputs were 38%, 36%, and 53%, compared to 37%, 33%, and 40% of RoW respondents. However, of note is the fact that a greater range of RoW respondents also preferred the manual redirection model (12% to 25%) versus their U.S. colleagues (9% to 19%).

Figure 45: Minimizing 5G Fraud: U.S. vs. RoW
U.S. (N=45-46)

	Extremely important	Important	Somewhat important	Not important
Real-time fraud control to cope with advanced fraud tools and campaigns	40%	40%	20%	0%
Decreasing poll time between event and CDR creation	35%	48%	15%	2%
Fraud monitoring – including white list support	35%	41%	22%	2%
IMSI - GTT correlation	31%	47%	18%	4%
CLI Monitoring	22%	59%	20%	0%
Protection against Wangiri fraud	29%	44%	22%	4%

RoW (N=51-54)

	Extremely important	Important	Somewhat important	Not important
Real-time fraud control to cope with advanced fraud tools and campaigns	34%	47%	17%	2%
Decreasing poll time between event and CDR creation	28%	53%	17%	2%
Fraud monitoring – including white list support	28%	57%	16%	0%
IMSI - GTT correlation	25%	51%	23%	2%
CLI Monitoring	30%	45%	21%	4%
Protection against Wangiri fraud	24%	46%	20%	9%

Question: How important are the following capabilities toward minimizing 5G fraud?
Source: Heavy Reading

Key Findings

There are some variances on specific data points, including the "importance" of fraud monitoring (U.S. 41% vs. RoW 57%). But overall, the two filter groups display similar data ranges across all four categories, which should serve them well in their global efforts to curb 5G fraud.

Figure 46: Implementing Automated Security Policy: U.S. vs. RoW
U.S. (N=47)

We will initially launch commercial 5G services with manual policy, utilizing additional staff and adopt automation over time.	38%
We will not commercially launch 5G services without automated security policy, but will not hire additional staff to facilitate the introduction	28%
We will not commercially launch 5G services without automated security policy, and will hire additional staff to facilitate the introduction	17%
Not sure, we are still studying our options.	13%
We will initially launch commercial 5G services with manual policy, utilizing existing staff and adopt automation over time.	4%

RoW (N=54)

We will initially launch commercial 5G services with manual policy, utilizing additional staff and adopt automation over time.	20%
We will not commercially launch 5G services without automated security policy, but will not hire additional staff to facilitate the introduction	22%
We will not commercially launch 5G services without automated security policy, and will hire additional staff to facilitate the introduction	26%
Not sure, we are still studying our options.	20%
We will initially launch commercial 5G services with manual policy, utilizing existing staff and adopt automation over time.	11%

Question: Which statement best reflects your automated security policy adoption strategy when deploying 5G networks?
Source: Heavy Reading

Key Findings

U.S. respondents prefer to launch 5G using a manual policy and hiring additional staff to facilitate the transition to automation (38%), while only 20% of RoW respondents consider this a viable approach. In contrast, RoW respondents tend to prefer to launch 5G with automated policy and additional staff (26%) compared to 17% of U.S. respondents. The more aggressive 5G rollout schedule of U.S. respondents and the availability of commercial automated policy products may be a factor in the decision process to launch with a manual policy. The other manual policy option, which advocated for no additional staff, did not really resonate with either group (U.S. 4% vs. RoW 11%).

Figure 47: Automation and OPEX: U.S. vs. RoW

U.S. (N=44-47)

	More than 25%	10% to 25%	Less than 10%
Securing the portals used by end-customers to manage policy in a slice	32%	49%	19%
Security for Public Cloud App/Services	23%	52%	25%
Security for Private Cloud Apps/Services	22%	53%	24%
Policies that control the security of traffic inside a slice	26%	50%	24%
Setting DDoS attack detection & mitigation thresholds	23%	53%	23%

RoW (N=51-53)

	More than 25%	10% to 25%	Less than 10%
Securing the portals used by end-customers to manage policy in a slice	16%	51%	33%
Security for Public Cloud App/Services	23%	46%	31%
Security for Private Cloud Apps/Services	19%	47%	34%
Policies that control the security of traffic inside a slice	15%	47%	38%
Setting DDoS attack detection & mitigation thresholds	17%	53%	30%

Question: What is the OPEX reduction potential for the following automated 5G security policy focus areas?

Source: Heavy Reading

Key Findings

U.S. respondents have a more bullish view of the OPEX-related savings associated with the implementation of automated security policy than their RoW counterparts based on the "more than 25%" range of responses (U.S. 22% to 32% vs. RoW 15% to 23%). Similarly, a greater number of RoW respondents forecast less than 10% OPEX savings (RoW 30% to 38% vs. U.S. 19% to 25%).

Figure 48: The Importance of Content Inspection: U.S. vs. RoW

U.S. (N=45-46)

	Extremely important	Important	Somewhat important	Not important
5G NR RAN	39%	41%	20%	0%
5G NGC Core	39%	46%	13%	2%
Roaming	31%	49%	18%	2%
Gi/SGi interface	31%	33%	33%	2%
MEC cloud	29%	44%	24%	2%

RoW (N=51-53)

	Extremely important	Important	Somewhat important	Not important
5G NR RAN	45%	38%	15%	2%
5G NGC Core	43%	45%	12%	0%
Roaming	32%	49%	19%	0%
Gi/SGi interface	19%	49%	32%	0%
MEC cloud	19%	56%	25%	0%

Question: How important is the application of full content inspection to gain insight into attacks, vulnerabilities, malicious URLs, and malware?

Source: Heavy Reading

Key Findings

Based on generally similar level "extremely important" and "important" responses, it is clear that both groups assess content inspection as a vital tool to assist them in attack and malware mitigation. For both groups, the areas by a considerable margin where content inspection was assessed as most important were in the RAN and NGC core (U.S. 39% and 39% vs. RoW 45% and 43%).

Figure 49: 5G Security Vendor Selection Criteria: U.S. vs. RoW

U.S. (N=44-46)

	Extremely important	Important	Somewhat important	Not important
Backward compatibility with existing mobility infrastructure	37%	46%	17%	0%
Pre-validated third-party integration certification	33%	48%	20%	0%
Vendor maturity and portfolio breadth	20%	62%	16%	2%
Existing account footprint	16%	56%	29%	0%

RoW (N=48-53)

	Extremely important	Important	Somewhat important	Not important
Backward compatibility with existing mobility infrastructure	40%	50%	6%	4%
Pre-validated third-party integration certification	19%	62%	15%	4%
Vendor maturity and portfolio breadth	26%	49%	23%	2%
Existing account footprint	15%	59%	15%	11%

Question: How important are the following factors when selecting 5G security vendors?

Source: Heavy Reading

Key Findings

Vendor engagements are often driven by unique geographical market forces. But based on the similarity of "extremely important" response trends and rankings, both groups possessed similar views on the relative weighting of the factors, including backward compatibility (U.S. 37% vs. RoW 40%) and existing account footprint (U.S. 16% vs. RoW 15%).

One area where a significant deviation level was noted was the value of third-party integration, which was viewed as "extremely important" by 33% of U.S. respondents, compared to only 19% of RoW respondents.

A number of factors are likely in play here. One plausible consideration is that because RoW networks rely more heavily on managed services, this requirement could be supported as part of an existing managed services agreement. Therefore, it is less important than the U.S. model, where carriers continue to be responsible for network operation and systems integration.

Figure 50: 5G Fraud and Signaling Security Vendor Selection Criteria: U.S. vs. RoW

U.S. (N=45-46)

	Extremely important	Important	Somewhat important	Not important
Flexibility - programmable rule sets to implement real-time defense against new attacks	41%	41%	17%	0%
Multi-tenant solution - NF protects against a wide variety of use cases	33%	59%	9%	0%
High volume data capabilities – NF can scale to handle high volume of data	28%	59%	13%	0%
API controlled solution - solution supports an HTTP REST interface for lean management	35%	52%	13%	0%
Supports a distributed architecture which provides the same level of protection independent of edge position and location of resources	38%	42%	20%	0%
Centralized data management - NF in the micro datacenter can be also be provisioned from a remote data center	22%	49%	29%	0%
Advanced programmable and graphical reporting support - easy to use KPI management and error diagnostic tools	23%	52%	25%	0%

RoW (N=52-53)

	Extremely important	Important	Somewhat important	Not important
Flexibility - programmable rule sets to implement real-time defense against new attacks	40%	48%	10%	2%
Multi-tenant solution - NF protects against a wide variety of use cases	45%	51%	2%	2%
High volume data capabilities – NF can scale to handle high volume of data	34%	45%	19%	2%
API controlled solution - solution supports an HTTP REST interface for lean management	24%	50%	22%	4%
Supports a distributed architecture which provides the same level of protection independent of edge position and location of resources	21%	58%	17%	4%
Centralized data management - NF in the micro datacenter can be also be provisioned from a remote data center	26%	47%	21%	6%
Advanced programmable and graphical reporting support - easy to use KPI management and error diagnostic tools	21%	48%	25%	6%

Question: How important are the following NF capabilities when selecting a 5G control plane vendor to support 5G and MEC signaling security and fraud protection?
Source: Heavy Reading

Key Findings

A considerable degree of alignment exists based on general data trends of both "extremely important" and "important" responses. For example, both groups essentially agreed that flexibility/programmable rule sets were an extremely important consideration (U.S. 41% vs. RoW 40%). But there were some notable differences as well.

While the top three extremely important factors for U.S. respondents were flexibility, distributed architecture support (38%), and API/REST support (35%), the RoW respondents' top three priorities were multi-tenant support (45%), flexibility, and high volume data-scale capabilities (34%).