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

HEAVY READING
WHITE PAPER

Implementing 5G Security: Priorities and Preferences

A Heavy Reading white paper produced for F5 Networks, Fortinet, NetNumber, and Palo Alto Networks

AUTHOR: JIM HODGES, PRINCIPAL ANALYST, HEAVY READING

INTRODUCTION

Today's cycle of provisioning live 5G networks constitutes the first steps of building a new era of mobile communications infrastructure. The scope of change inherent with 5G network design and operation is profound and extends well beyond simply deploying a new radio access network (RAN) or core network. Unlike previous generations, 5G marks the first deployment of natively designed cloud-based network infrastructure that future generations of mobile technology will rely upon to support the challenging demands of new services targeting personal care, logistic services, automotive, and virtual reality gaming.

The same is also true from a 5G security enforcement perspective. To flourish in this new operational model, communications service providers (CSPs) must commit to adopting new security strategies, deploying new products, and even developing new monetization models to fully address the new security wrinkles 5G presents.

Heavy Reading, in collaboration with research sponsors F5 Networks, Fortinet, NetNumber, and Palo Alto Networks, launched the *5G Security Market Leadership* study to fully understand the scope of the security implications. This study was based on a comprehensive survey that was deployed in 1Q 2019. The survey attracted 103 global survey respondents who worked for a cross-section of carriers of various sizes.

This white paper presents a subset of several key findings from the study that provide valuable security-related insight into investment priorities, architecture preferences, and control plane considerations. It also assesses the value of implementing advanced capabilities such as content inspection and automated security policy enforcement.

5G SECURITY USE CASE INVESTMENT PRIORITIES

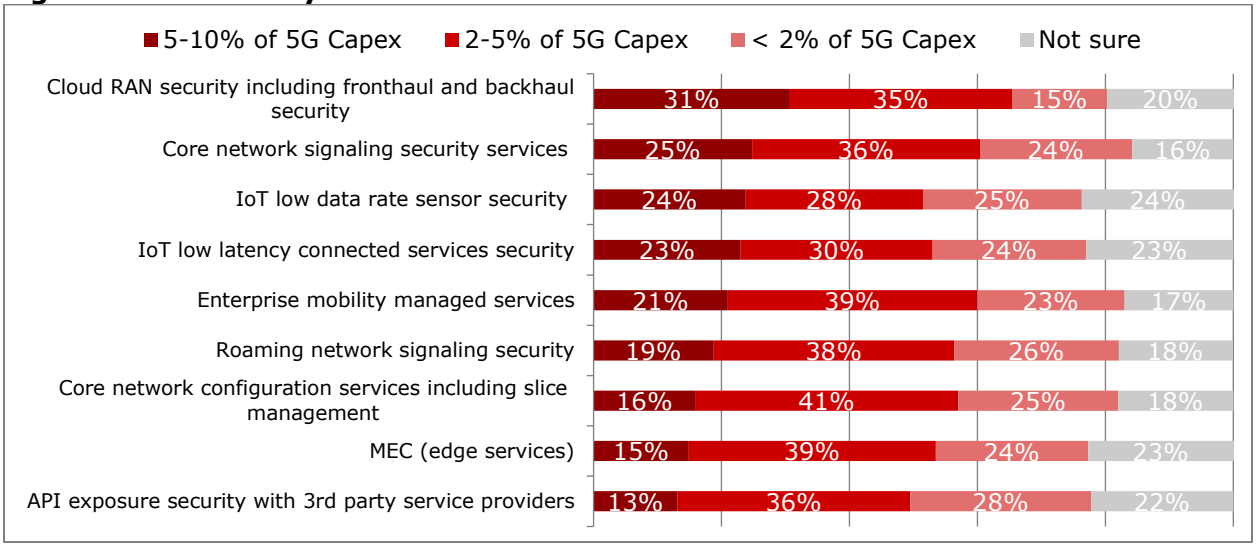
Over the past 18 months, the managed security services market has experienced strong growth as the pace and complexity of mobile threat vectors have increased. The relative value proposition of mobile security managed services is likely to increase with the widening of attack surfaces that 5G will fuel. Several factors will drive this flaring. These include functional separation of the 5G New Radio (NR) with new backhaul and fronthaul interfaces and the deployment of the fully distributed, slice-enabled, and decoupled internet-based signaling control plane of the 5G next-generation core (NGC).

In response to this threat landscape expansion, CSPs are planning to continue to invest in managed security services to address a broad range of areas where threats could be encountered. But even looking ahead 3-5 years after commercial deployment, as shown in **Figure 1**, the top two priorities that will attract the greatest levels of security managed services capex investment (5%-10% of 5G capex) will still be the RAN and core. Cloud RAN security stood out as the top investment priority (31%), followed by core network signaling security services (25%).

It is also worth noting that a significant range of respondents (16%-24%) remain unsure of their managed security services investment priorities, suggesting capex allocation for 5G security services is still relatively fluid. This is not too surprising, given that not all 5G use cases will be supported at launch. In addition, with any transformation of this magnitude,

the reality is that not all services/use cases will be widely accepted or attain sustainable business models.

Figure 1: 5G Security Use Case Investment Priorities



Question: How much will you invest in the following use cases 3-5 years after 5G commercial deployment? (N=99-101)
Source: Heavy Reading 5G Security Market Leadership Study, January 2019

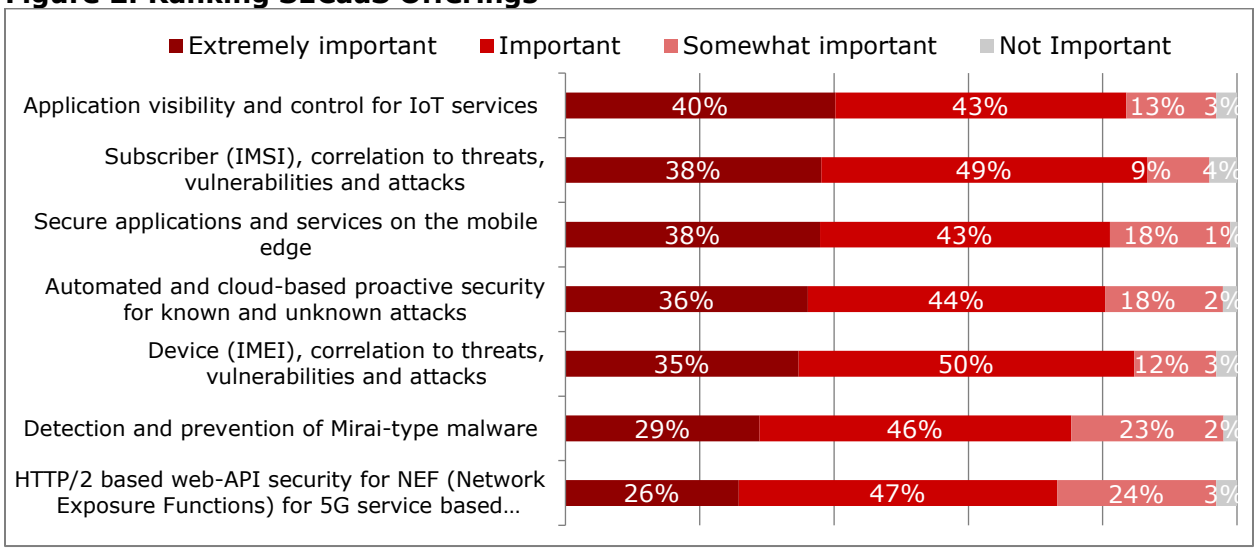
One of the considerations associated with achieving a sustainable business model is understanding on a granular level specific market requirements for cloud-based security services such as security as a service (SECaaS).

Based on the close ranking of "extremely important" responses captured in **Figure 2**, it is apparent that CSPs consider several key functions as vital to enhancing their SECaaS offerings. At the top of the list is application-level visibility for Internet of Things (IoT) services (40%) to offer deep visibility and granular control even inside mobile tunnels. This is followed closely by subscriber/IMSI threat correlation and secure applications on the mobile edge (both 38%). Next are automated cloud security (36%) and device/IMEI correlation to threats (35%). Utilizing both International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) threat correlation enables CSPs to identify infected subscribers and devices for faster security troubleshooting.

While HTTP/2 application programming interface (API) security for Network Exposure Function (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. Accordingly, a key conclusion here is that the survey respondents understand that successful SECaaS

delivery must be bolstered by a number of strategically important and powerful automated security capabilities.

Figure 2: Ranking SECaaS Offerings



Question: How important are the following 5G SECaaS offerings? (N=95-98)
Source: Heavy Reading 5G Security Market Leadership Study, January 2019

5G SECURITY ARCHITECTURE PREFERENCES

Although the cloud technology will dominate the future, it will take years to fully build out 5G networks and sunset existing networks. This means CSPs must be adept at running security policies in a hybrid network configuration to support secure fallback scenarios and roaming.

Therefore, one of the key decisions that CSPs must make well before 5G commercial launch is which core network to utilize. Essentially, 5G networks can be launched using two configurations. Non-standalone mode (NSA) pairs the 5G NR RAN with the existing 4G core, while the standalone mode (SA) implements both the 5G NR and the 5G NGC.

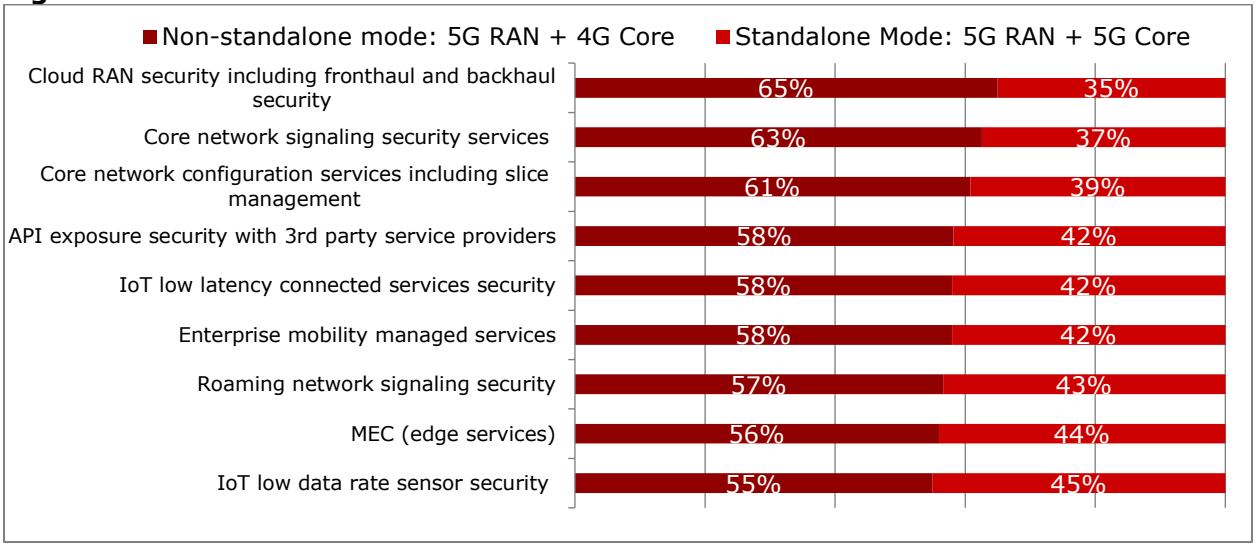
Although the SA option is positioned as the end game since it facilitates advanced capabilities, such as API exposure with third parties, and slice-based use cases, it also injects considerably more security complexity to service launch. Therefore, understanding CSP core launch preferences is important to fully document the breadth of security implications.

The results shown in **Figure 3** confirm that a majority of CSPs (55%-65%) plan to launch the common set of security use cases utilizing 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 implementing NSA also simplifies and pushes out the requirement to support 5G roaming on IP exchange (IPX) networks. Adoption of NSA also

reduces complexity for evolving enterprise managed security services, which have experienced strong growth over the past few years.

Figure 3: 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 5G Security Market Leadership Study, January 2019

As a distributed cloud-based architecture with newly defined interfaces, 5G will need to support traffic encryption. Therefore, understanding encryption preferences in various layers of the network is important to appreciate the end-to-end security implications like the procedures for key management and traffic visibility for network inspection and control.

Focusing on the RAN, core, and edge, **Figure 4** indicates the preferred approach in the radio network is to implement IP Security (IPSec) protocol-based encryption (54%). 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 utilize the Transport Layer Security (TLS) protocol-based approach (including supporting the TLS based Datagram Transport Layer Security [DTLS] option). These options garnered solid support metrics ranging from 25% in the RAN to 34% facing the core (backhaul interfaces) and 31% core facing the internet. One factor in the support of TLS may be related to a recent upgrade. A new version of TLS (1.3) released in 3Q 2018 by the Internet Engineering Task Force (IETF) supports new security and performance capabilities by expanding encryption support and eliminating support of older, less secure algorithms.

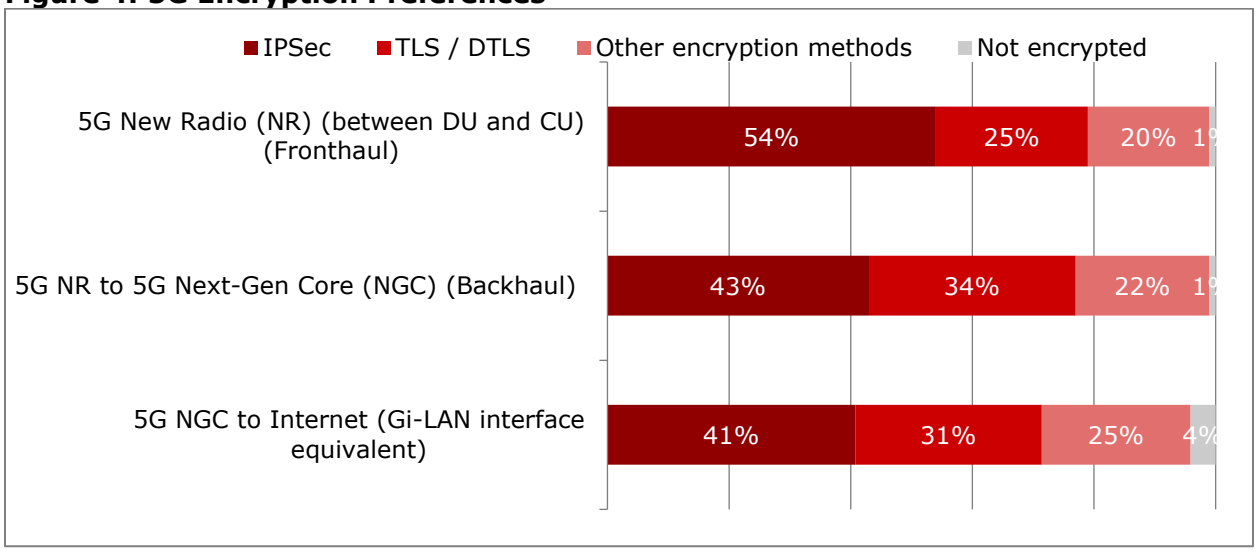
Somewhat surprisingly and higher than Heavy Reading expected was the level of support of the "other" encryption methods. This fell into the 20% range in the RAN to a high of 25% for core internet-facing interfaces.

These inputs may have been influenced by ongoing discussions and interest in using alternative encryption approaches such as the Quick UDP Internet Connection (QUIC) protocol

developed by Google to optimize management of HTTP/2 services in a low latency environment, which aligns with the new 5G core model.

The positive news is that only a very small subset of respondents (4% or less) advocated not using encryption.

Figure 4: 5G Encryption Preferences



Question: What is your preferred encryption choice for securing data on the following network layers? (N=98-100)
Source: Heavy Reading 5G Security Market Leadership Study, January 2019

THE CONTROL PLANE CONUNDRUM

While the signaling control planes of 2G/3G and 4G networks have proven themselves highly reliable, 5G amps up the complexity and threat level on the control plane. Consequently, 5G will dictate new approaches to meet these more complex security demands.

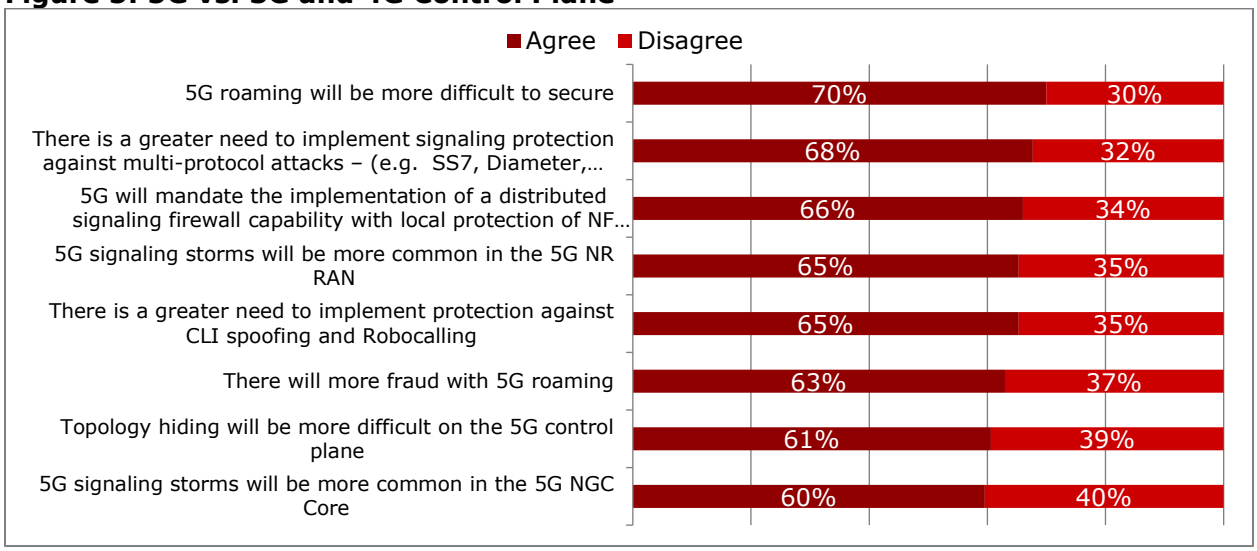
As shown in **Figure 5**, CSPs understand that things are different with 5G and that new challenges will be encountered. There are numerous takeaways here based on the percentage of "agree" responses in the figure.

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 believe that signaling storms will be more common both in the NR and NGC (65% and 60%).

These factors also mean that to fully address the control plane security conundrum, CSPs must be able to protect against multiprotocol attacks (68%), which will drive the deployment of distributed signaling firewalls (66%). Such firewalls are strategically important because they address topology hiding challenges (61%) and improve responses

to threat vectors utilizing calling line identifier (CLI) spoofing and robocalling (65%), as well as mitigate the impact of fraud (63%).

Figure 5: 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 5G Security Market Leadership Study, January 2019

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

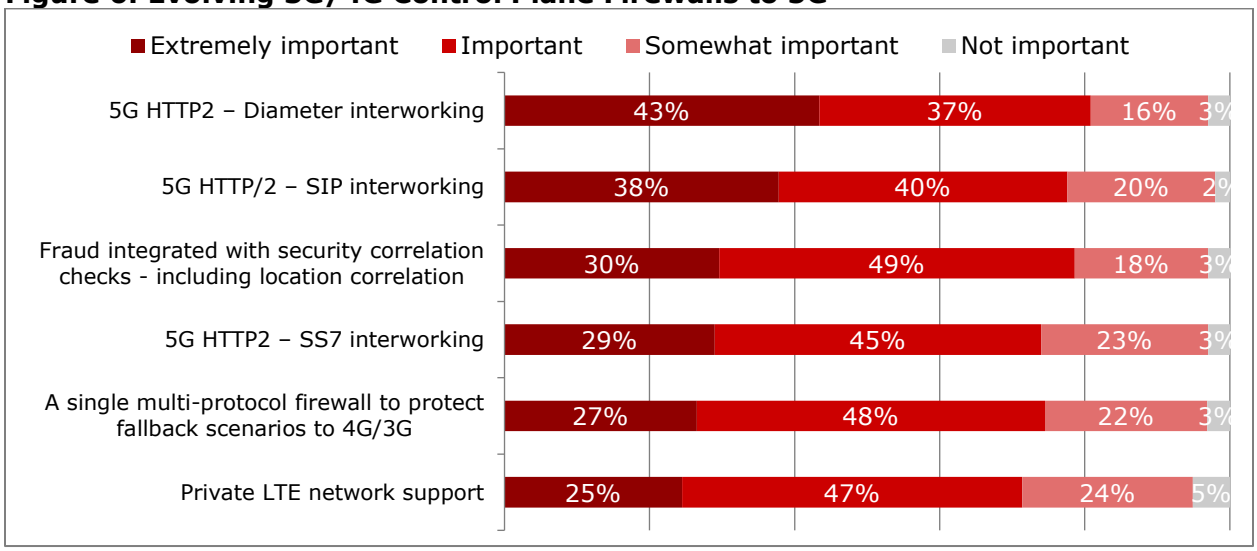
An important consideration in this process, as touched upon above, is the extent to which existing 3G and 4G control plane firewalls can evolve to support 5G. **Figure 6** provides valuable insight into which capabilities the respondents consider most important in this journey.

While all the attributes listed in the question had significant levels of support, based on "extremely important" inputs, the respondents tended to gravitate toward HTTP/2 – Diameter interworking (43%), HTTP/2 – SIP interworking (38%), and then fraud/correlation capabilities (30%). These were followed by HTTP/2 – SS7 interworking (29%) and single/multiprotocol support firewall (27%), which reflects the need to support HTTP/2 Diameter, Session Initiation Protocol (SIP), and even Signaling System 7 (SS7) interworking.

The level of "important" responses (37%-49%) are also significant and reaffirm the need to enhance the security focus on 5G fraud mitigation (49%) and deploy a single multiprotocol

firewall (48%). They also stress the importance of ensuring firewalls can support private Long-Term Evolution (LTE) networks (47%), which continue to gain market traction.

Figure 6: 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 5G Security Market Leadership Study, January 2019

THE WAY FORWARD

Another of the 5G security realities that CSPs must address is the requirement to implement real-time security policy capable of responding in the low latency speeds 5G supports.

Generally, the industry has already accepted that the only viable long-term option for implementing real-time security policy is to *automate* real-time security policy. Accordingly, the survey investigated the pace of implementing automated security policy as well as the staffing implications. The data inputs shown in **Figure 7** captured support for several approaches.

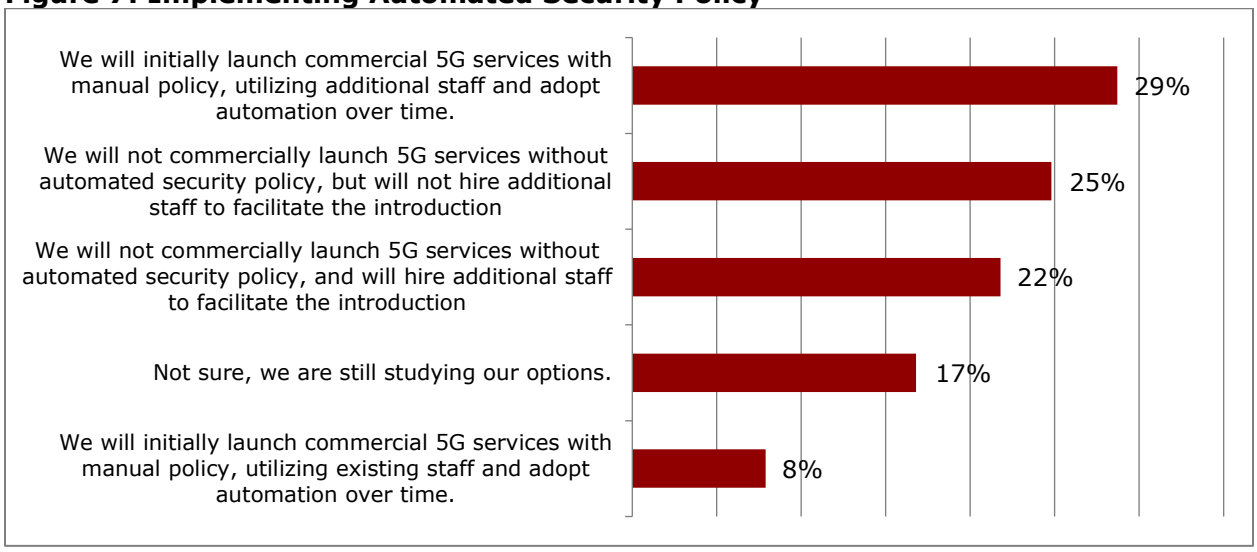
The most common sentiment among the respondents by a slight margin was that CSPs would launch commercial 5G services utilizing manual policy with additional staff and adopt automation over time (29%) as more markets rolled out. Another group advocated a similar approach in terms of support for a manual policy launch, but this smaller group (only 8% of respondents) adopted the status quo approach of utilizing manual policy with existing staff.

In contrast, two other groups would not launch commercial service without automated security policy. Of these, the slightly larger of the two would not hire additional staff (25%) while the other group that would hire additional staff to facilitate the rollout (22%).

Based on the response rates of these two groups, almost half of the respondents (25% + 22% = 47%) appear committed to implementing automated security policy at launch compared to 37% who advocate a manual-only launch (29% + 8% = 37%).

Based on this input, while day one support of automated policy may not be overwhelming, the identification by almost half of the respondents that 5G must be automated at commercial launch reinforces the notion that automated security policy represents the way forward and that maintaining a status quo strategy is not realistic option.

Figure 7: Implementing Automated Security Policy



Question: Which statement best reflects your automated security policy adoption strategy when deploying 5G networks? (N=101)
Source: Heavy Reading 5G Security Market Leadership Study, January 2019

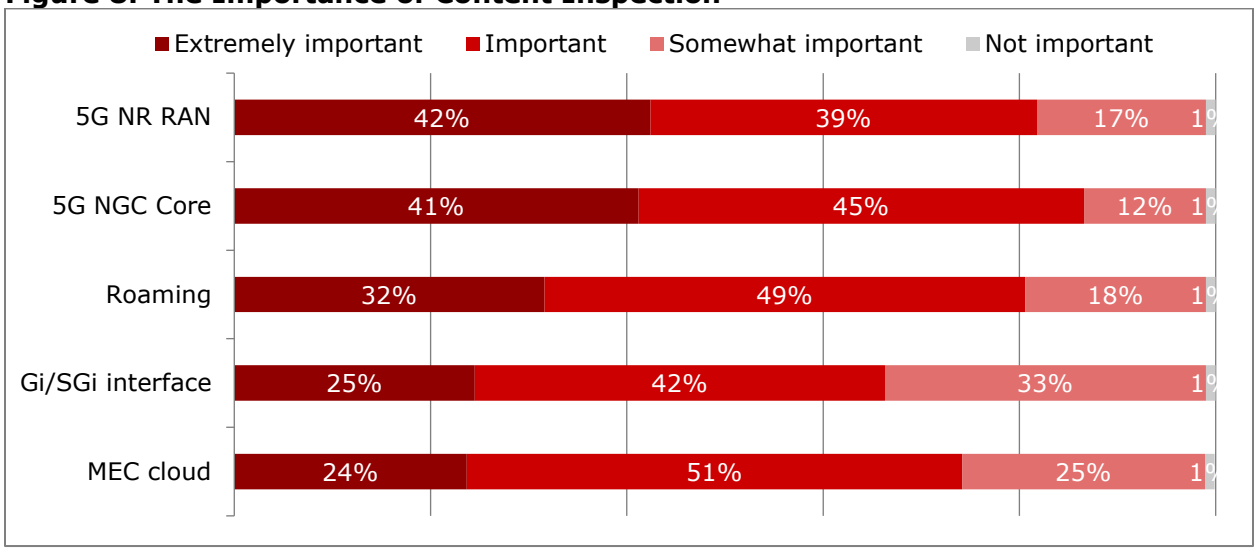
Another capability that is often positioned as crucial for securing 5G networks is content inspection. While the concept of inspecting content running over mobile networks is not new, the introduction of 5G network slices and the further distribution of software to run at the edge changes the dynamic of where and how security enforcement is invoked.

As a result, the value of content inspection as a tool to provide enhanced insight into 5G realm attacks is noted in a few places in the survey. But **Figure 8** serves to close the feedback loop in the context of the RAN and core, where 42% and 41% of respondents assessed content inspection as "extremely important." The takeaway is that the enhanced level of visibility in RAN and core afforded by content inspection is fast becoming a strategically important "must have" network security capability.

Furthermore, while the percentage of "extremely important" responses drops off for roaming (32%), implementing on the Gi-LAN (25%), and mobile edge computing (MEC; 24%), the strong proportion of "important" responses for these three (49%, 42%, and

51%, respectively) validates the idea that content inspection is a valuable threat mitigation tool on many levels.

Figure 8: 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 5G Security Market Leadership Study, January 2019

CONCLUSION

The research contained in this white paper, in conjunction with the key findings from the entire *5G Security Market Leadership* study survey, confirm that CSPs are in the early phase of a generational shift that will dramatically alter how they will secure their networks.

Many CSPs have already defined security use case implementation priorities and even architecture preferences. However, the research also confirms that resolving the formidable security challenges that await will mandate embracing new technologies to ensure successful outcomes during the all-important implementation phase.