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

HEAVY READING
WHITE PAPER

Standalone Security:
Adoption, Automation, Attributes, and Attacks

A Heavy Reading white paper produced for A10 Networks, Ericsson, Hewlett Packard Enterprise, and NetNumber

AUTHOR: JIM HODGES, CHIEF ANALYST, HEAVY READING

INTRODUCTION

5G is already a commercial reality in many global markets that have deployed 5G radio access networks (RANs) paired with a 4G core. But it is now poised to take a second and vital step that will fully unlock the value of communications service providers' (CSPs') 5G network investment. This step is the deployment of the 5G core (5GC), which constitutes a breakthrough from previous mobile core network generations in terms of both performance and service support.

The pairing of the 5GC and 5G RAN, referred to as a standalone (SA) configuration, represents a blank canvas from a service delivery perspective. 5GC services utilize a cloud-native microservices design that leverages the power and reach of an API exposure model.

In addition, this architecture is designed to run these services in a fully decentralized configuration at the network edge, which enables a major reduction in application latency. The 5GC also supports the ability to create distinct software slices that can be utilized to create high performance, high value tailored services.

However, support of these new services and capabilities, including the broader distribution of necessary functions to the edge, has profound security implications. CSPs must address these issues to ensure 5G performance and service gains are not undermined by opportunistic security threats such as distributed denial-of-service (DDoS) attacks.

In response, Heavy Reading, in collaboration with research sponsors A10 Networks, Ericsson, Hewlett Packard Enterprise, and NetNumber, launched the *5G Core Security Market Leadership* study. It was designed to provide granular insight into the scope of the security implications associated with shifting to the 5G SA architecture. Deployed in 3Q20, this study utilized 32 questions and attracted 115 global survey respondents who worked for a cross-section of carriers of various sizes.

This white paper presents a subset of several key data points from the study addressing the 5G SA core adoption timeline and the security attributes that CSPs must consider in formulating effective security strategies.

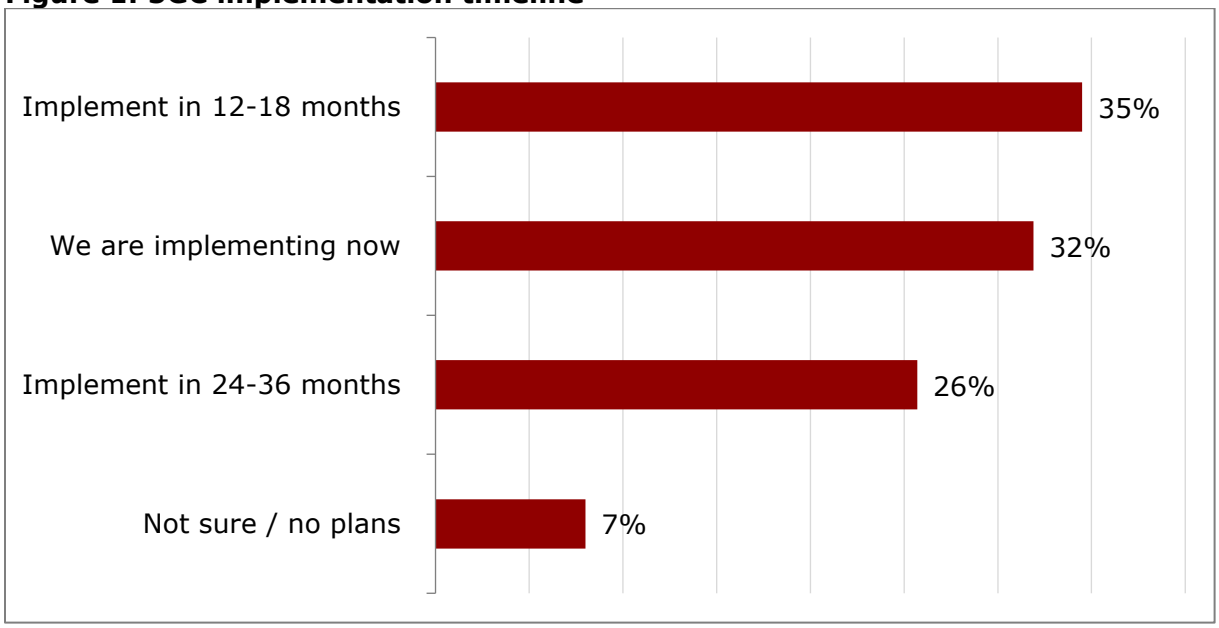
ADOPTION, ATTRIBUTES, AND AUTOMATION

The commercial implementation of the 5GC represents a vital step in migrating to a fully cloud-based mobile network. However, deployments will take place over the next five years to minimize network risk and capex investment while continuing to maximize the revenue potential of existing 3G and 4G networks.

Still, as shown in **Figure 1** below, many CSPs have initiated processes that will fuel the adoption curve. Of these, 32% have already started the implementation process while another 35% plan to start implementing in 12–18 months. An additional 26% forecast implementation taking place in a 24- to 36-month window.

This equates to 67% (32% + 35%) of respondents expecting to have some form of 5GC SA implemented in some parts of their networks within an 18-month window. And 93% expect to implement within a 36-month window (35% + 32% + 26%), validating that almost all CSPs consider SA implementation a strategic imperative.

Figure 1: 5GC implementation timeline



Question: When do you plan to implement a 5G core (5GC) in a standalone mode (SA) configuration? (n=113)
Source: Heavy Reading

As these deployments scale and 5GC inherent service capabilities such as slicing and API exposure are activated in live networks, a general anecdotal concern is that new more complex and potent threat vectors and attack scenarios will also be encountered.

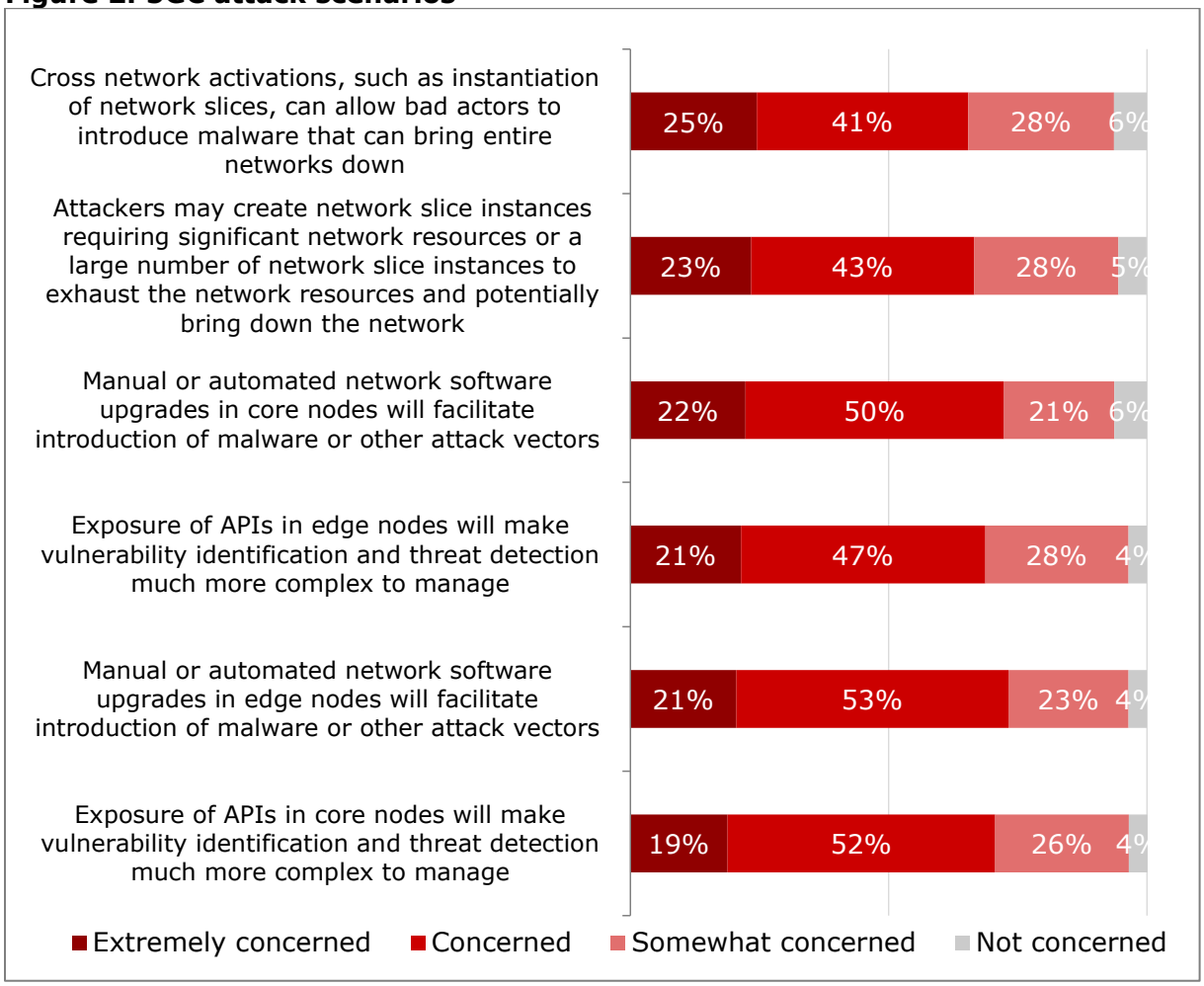
According to survey respondents, 5GC attack scenarios of most concern are based on external triggers and of less concern are the internal control points. This is a logical outcome given the fact that external actors are less predictable and therefore demand a more sophisticated defense than for internal control points.

This viewpoint is validated in **Figure 2** below. Based on "extremely concerned" inputs, cross-network activations raise the most concern (25%). This relates to slice-based malware and similarly may point to the signaling interfaces for roaming support with other 5GC networks worldwide.

Attacker created slice instances (23%) is the second leading attack scenario of concern. API exposure in edge and core nodes (21% and 19%) and the introduction of automation-based software upgrades (22% and 21%) also constitute sources of apprehension.

The key finding here is clear: the introduction of API exposure, automation, and sliced-based services injects formidable challenges that must be fully addressed before 5GC and distributed edge implementation.

Figure 2: 5GC attack scenarios



Question: The 5GC will introduce new requirements. How concerned are you the following scenarios will impact your ability to secure the 5GC network? (n=110–112)
Source: Heavy Reading

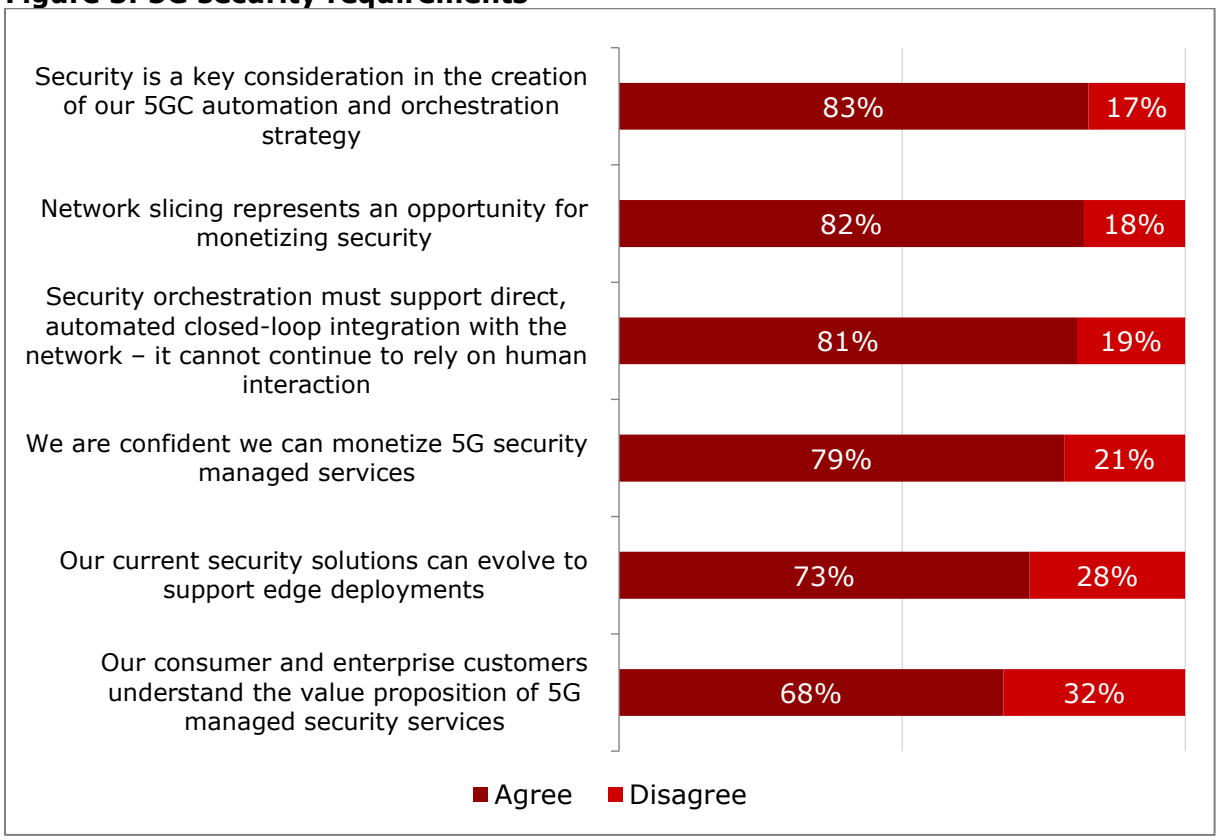
While slicing, API exposure, and automation inject additional complexity into 5G security strategy execution, a vast majority of CSPs also see a business opportunity to upsell or monetize security services.

For example, as **Figure 3** below captures, based on "agree" inputs, 68–83% of survey respondents believe security-related opportunities also exist. Of these, the leading opportunity is to utilize security as a key attribute in the creation of a 5GC automation and orchestration (83%) strategy.

Furthermore, a high percentage of respondents agree that network slicing represents an opportunity to monetize security (82%) and that security orchestration must shift away from manual processes to automated processes (81%). This makes sense given microservices run in containers that utilize an automated orchestrator to manage and scale workloads.

Not only does this input reaffirm the value of network slicing, orchestration, and automation, it also closes the feedback loop by validating that all three are not disparate concepts. Rather, they are synergistically integrated components of a viable and monetizable 5GC security strategy.

Figure 3: 5G security requirements



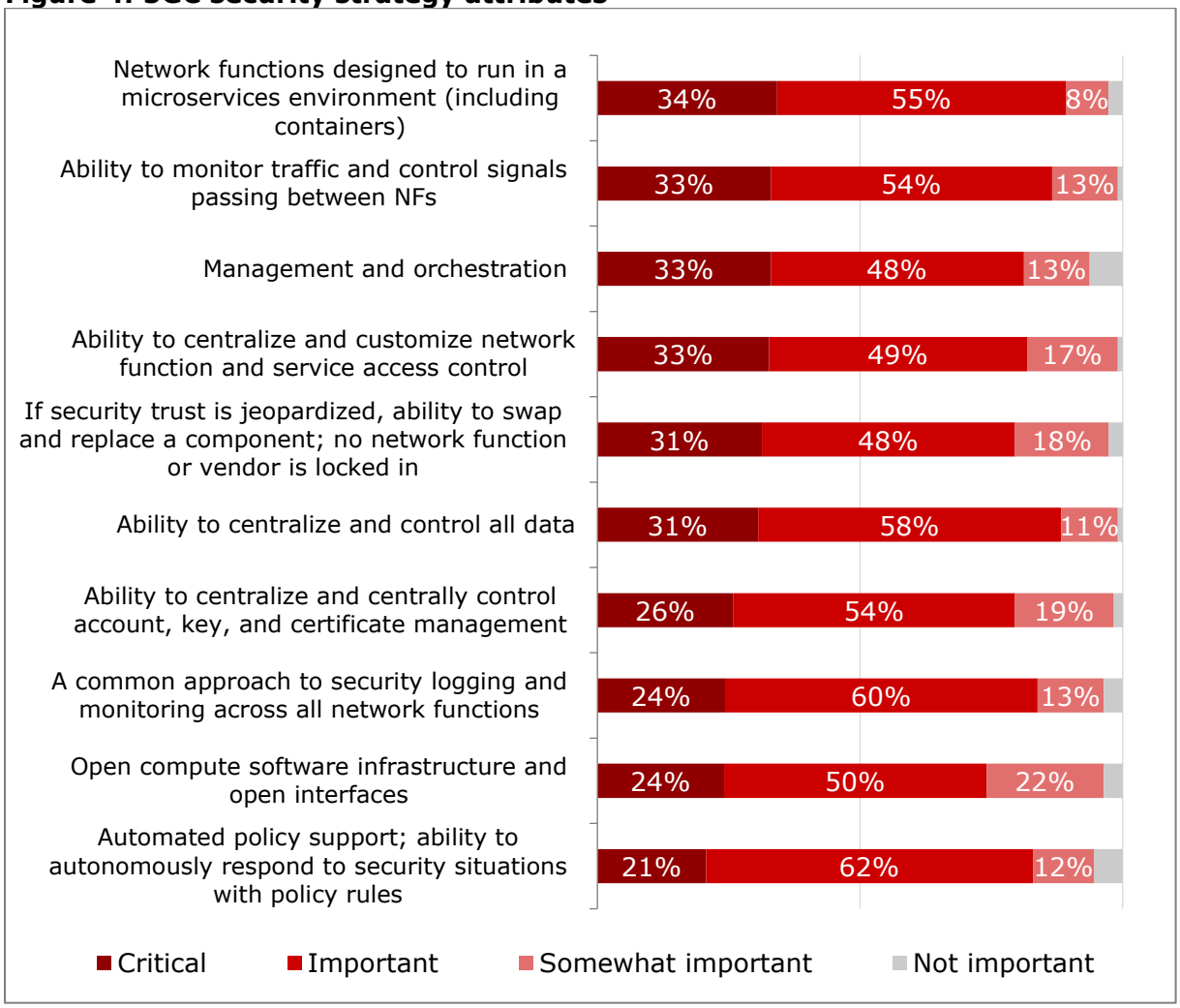
Question: Do you agree or disagree with the following statements? (n=109–112)
Source: Heavy Reading

Yet, it is important to note, as shown in **Figure 4** below, that along with network slicing, automation, and security orchestration, several other key attributes also form part of a comprehensive 5GC security strategy.

Based on "critical" inputs, additional attributes here include the ability to monitor traffic and control signals between network functions (33%), centralized and customizable network function and service access control (33%), swappable open platforms that avoid single-vendor lock-in (31%), and centralized data control (31%). Other open network-related attributes such as open software and interfaces also factor into the equation (24%).

Heavy Reading interprets this input as confirming that a viable 5GC security strategy must consider attributes beyond microservices support, orchestration, monitoring, and slicing and also address software programmability and hardware openness. The latter two attributes will enable CSPs to deliver the requisite level of flexibility to respond to the new threat landscape.

Figure 4: 5GC security strategy attributes



Question: Please rate the importance of the following attributes to your 5G core network security strategy. (n=110–112)
Source: Heavy Reading

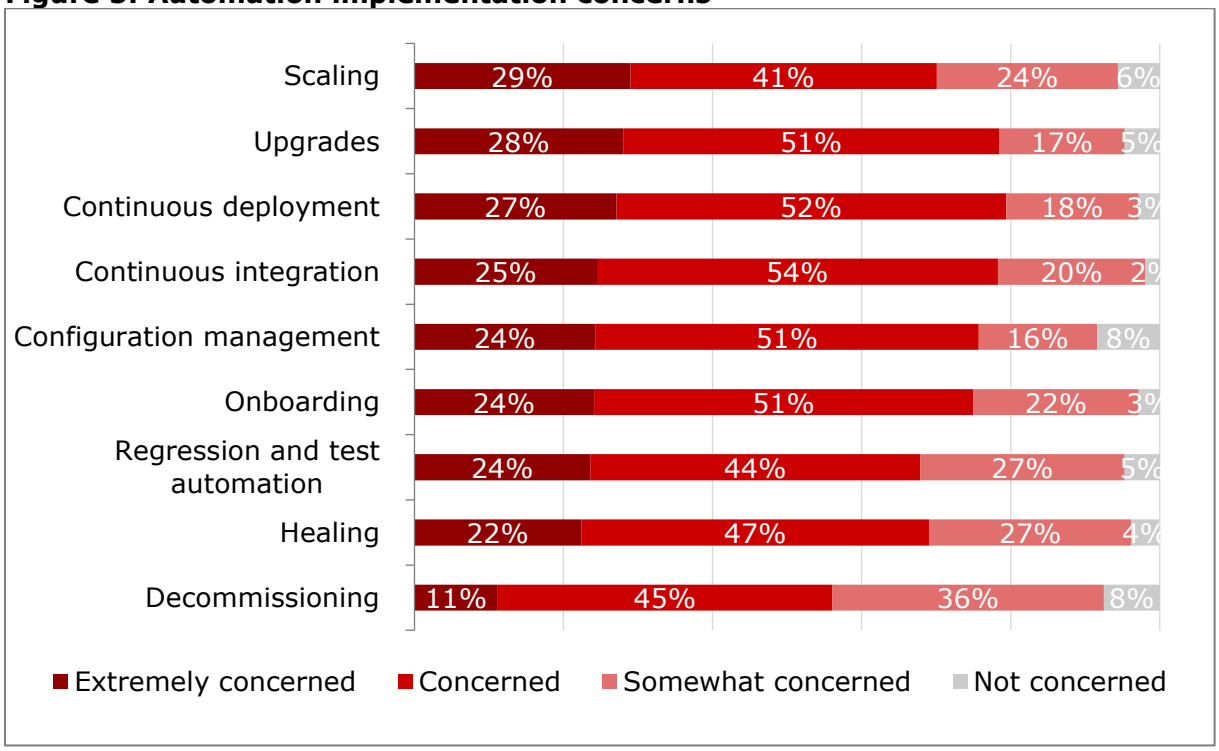
Automation is clearly a key construct of an effective 5GC security strategy. However, since it represents a major change to CSPs' existing operational procedures, automation introduces unique implementation concerns.

As **Figure 5** below illustrates, based on "extremely concerned" response levels, there are numerous concerns. Of these, scaling (29%), upgrades (28%), continuous deployment (27%), and continuous integration (25%) have the highest percentage of responses.

This was not unexpected given that mass adoption of automation on this scale has not been undertaken before. However, it does show that CSPs anticipate a broad range of complex implementation challenges.

Heavy Reading believes that this is one factor why these same CSPs identified the ability to swap out network components without vendor lock-in as well as open interfaces (shown in **Figure 4**) as important attributes to provide the greatest measure of automation scale and upgrade implementation flexibility.

Figure 5: Automation implementation concerns



Question: How concerned are you that deploying automation in 5GC networks to support the following orchestration, software upgrades, auto scaling, and self-healing capabilities will be complex and difficult to implement? (n=106–108)
Source: Heavy Reading

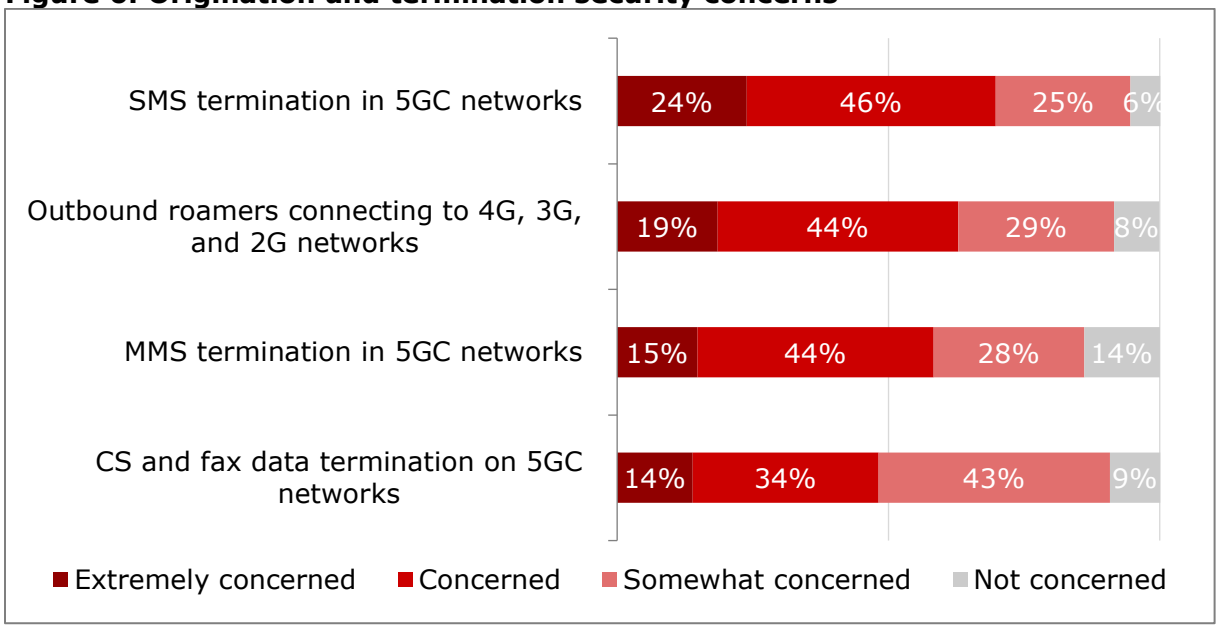
In addition to managing the inherent security complexities of 5G SA services, CSPs must also ensure that their 5G core network can support seamless handover and roaming with 2G, 3G, and 4G core networks. This is vital since mobile subscribers expect a seamless service model, including support of traditional services such as short messaging service (SMS) and multimedia messaging service (MMS), which date back to the 2G era.

As shown in **Figure 6** below, there are numerous execution-related apprehensions. Of these, based on "extremely concerned" and "concerned" responses, the top three concerns are SMS termination in 5GC networks (24% + 46%), outbound roaming (19% + 44%), and MMS termination in 5GC networks (15% + 44%).

Concerns with SMS, MMS termination, and roaming were expected since all three capabilities continue to be heavily utilized in the 5G era. At the same time, these rankings confirm there are formidable security concerns associated with 5GC legacy service support that must also be addressed in 5G SA security strategies.

Addressing these security concerns may demand the continued deployment of SS7 and Diameter signaling firewalls for the protection of 5G users to securely cover the seamless handover and roaming with the 2G,3G, and 4G core networks locally and worldwide.

Figure 6: Origination and termination security concerns



Question: How concerned from a security perspective are you about continuing to support the following services that originate or terminate on the 5GC SA? (n=108–109)
Source: Heavy Reading

RISE OF THE MULTI-ACCESS ATTACK LANDSCAPE

Along with factoring in security for legacy services, CSPs must also consider the impacts of multi-access edge computing (MEC)-based services. MEC is very similar to 5G in that it utilizes an edge-compute model based on microservices. However, it does not strictly rely on the 5GC core and can be implemented by deploying virtualized software applications running on open servers close to the subscribers in both fixed and mobile networks. This means MEC services can be supported by a 4G virtualized core network if it supports control and user plane separation.

As a result, MEC is also a topic of interest for many converged operators since it presents another revenue opportunity to upsell high value, low latency services. As a proof point, when Heavy Reading asked survey respondents to estimate MEC traffic as a portion of total traffic at the end of 2020, only 3% estimated their MEC network would carry 25–50% of traffic while 0% believed their MEC implementation would carry between 50% and 100% of traffic.*

* These data points were taken from the *5G Core Security Market Leadership study* and are not reflected in Figure 7.

By year-end 2025, MEC traffic level estimates transition to 13% of respondents in the 25–50% range and 8% in the 50–100% traffic range.[*] Although this growth is gradual, it injects an additional variable in the already complex decision process to allocate security investment across 4G, 5G, and MEC networks to protect critical network resources from a variety of distinct multi-access threat types.

The outcome of this investment balancing across multiple technologies, including MEC, is reflected in **Figure 7** below. To assess relative balance levels, the survey asked respondents to rank investment from highest (Rank 1) to lowest (Rank 4) by mobile technology (4G core, 5G non-standalone [NSA], 5G SA, and MEC) for various specific attack types.[†]

Overall, Rank 1 data input confirms that CSPs are following a balanced approach in terms of 4G and 5G core investment to address network-level threats. **Figure 7** also documents that investment varies not only by threat type, but also by where it is encountered in the network.

For example, in examining Rank 1 input related to threats from interconnecting roaming partners, the 4G core attained the highest ranking (34%) compared to MEC at 13%. This is logical since the 4G core today carries most roaming traffic.

But if the focus shifts to other attack types such as DDoS attacks, investment priorities change. In the case of small DDoS attacks targeting MEC nodes, MEC logically attained the highest level of Rank 1 investment input (39%) versus the 4G core (18%).

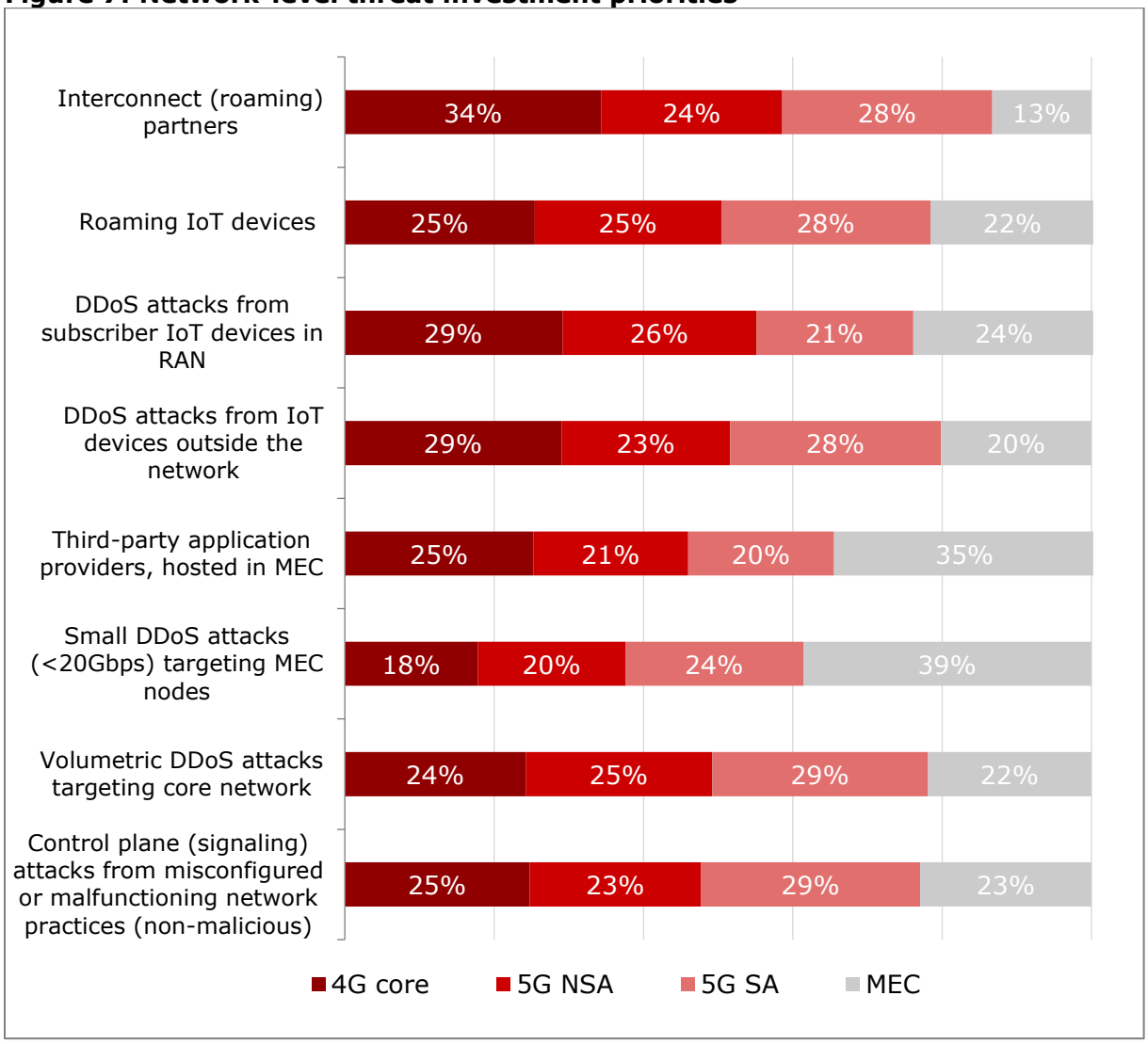
Moreover, the high range of Rank 1 scores for the 5G SA option for a variety of threat types (20–29%) confirms that considerable investment will be made in the 5G SA core to prepare it to scale and address the unique 5GC security threats shown in **Figure 2**. This includes control plane investments to address non-malicious attacks from misconfigured or malfunctioning devices or practices, which are of greater concern in 5GC (29%) than prior generations.

The message from all these data trends is clear. Investment must be made across all these generations of mobile technologies since they will all continue to face threat vectors that (if successful) will result in serious network outages.

[*] These data points were taken from the *5G Core Security Market Leadership study* and are not reflected in Figure 7.

[†] Only Rank 1 data is included in Figure 7.

Figure 7: Network-level threat investment priorities



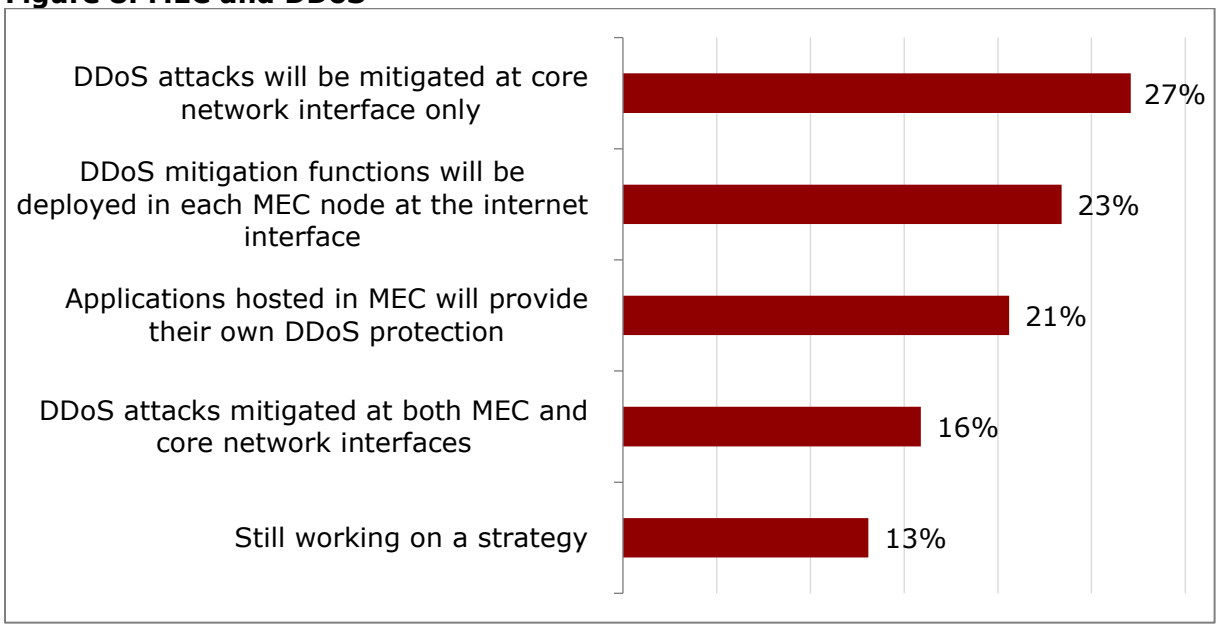
Question: On a scale of 1 to 4 where 1 is the greatest priority and 4 is the lowest priority, please rank your investment priorities in 4G, 5G, or MEC networks to address the following security threats: network-level threats. (n=111)
Source: Heavy Reading

Another consideration that affects investment allocation beyond network type is determining the interfaces on which the threat be mitigated. Utilizing a MEC network DDoS attack scenario as an example, several possible approaches can be implemented depending on DDoS-specific design attributes.

For instance, as shown in **Figure 8** below, while 27% of the survey respondents plan to protect MEC nodes from DDoS attacks via core network interfaces (including 5GC), 23% will deploy DDoS mitigation functions in each MEC node monitoring internet interfaces.

A third approach is to develop DDoS monitoring and mitigation protection in the application layer (21%) itself. This is logical given that DDoS attacks manifest themselves in various forms (e.g., application-layer attacks and volume-based attacks), but it reinforces that a flexible DDoS strategy is necessary at the edge.

Figure 8: MEC and DDoS



Question: How will MEC nodes be protected from DDoS and other attacks? (n=107)
Source: Heavy Reading

CONCLUSION

The research contained in this white paper and other complementary survey data points from Heavy Reading's *5G Core Security Market Leadership* study confirms that while CSPs are committed to the rollout of the 5G SA core, this adoption will ineradicably change security network enforcement fundamentals.

To prosper in this 5GC SA security service environment, CSPs will need to embrace several key principles. These include automation adoption and the implementation of open hardware, software, and orchestration solutions.

In parallel, CSPs must also remain committed to seamless interworking with the existing control plane and user plane security measures implemented in 2G, 3G, and 4G networks designed to secure both home network and roaming services. This will require a balanced security investment approach across multiple network technologies in centralized core and distributed MEC nodes to ensure that there is an adequate level of protection against existing threat vectors.

CSPs pragmatically anticipate complexity-driven challenges related to scaling, integrating, and updating these new SA security capabilities. However, the encouraging news is that they also anticipate 5GC SA adoption will enable them to expand their portfolio of security services, thereby solidifying customer relationships in the cloud.