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

HEAVY READING
WHITE PAPER

5G Security Strategy Considerations

A Heavy Reading white paper produced for Juniper Networks

AUTHOR: JIM HODGES, CHIEF ANALYST, HEAVY READING

INTRODUCTION

5G promises to be a game changer on several levels. 5G is not just about network speed, but also about enabling a diverse new set of services and vertical applications, including support for Internet of Things (IoT)-based applications. Significant innovation and design for RAN, core, and transport architectures have been completed. However, security remains a top concern for service providers as they create 5G evolution strategies and factor in the security impacts of unique device and application requirements.

Security is fundamental to the successful delivery of 5G networks across a wide range of industry verticals. 5G networks will connect substantial amounts of devices and serve different applications and customers with different security needs. The diversity of 5G applications and their scale, throughput, and latency requirements make it challenging to balance the efficiency, consistency, and accuracy of security management and security policies. In addition, the adoption of multi-access edge computing (MEC), virtualization, control-user plane separation (CUPS), and network slicing creates new attack surfaces that service providers must address.

This white paper documents what is fundamentally new about 5G, the security implications of 5G, and the security-related challenges and opportunities for service providers as they make the transition to 5G.

5G – WHAT'S NEW COMPARED TO 4G?

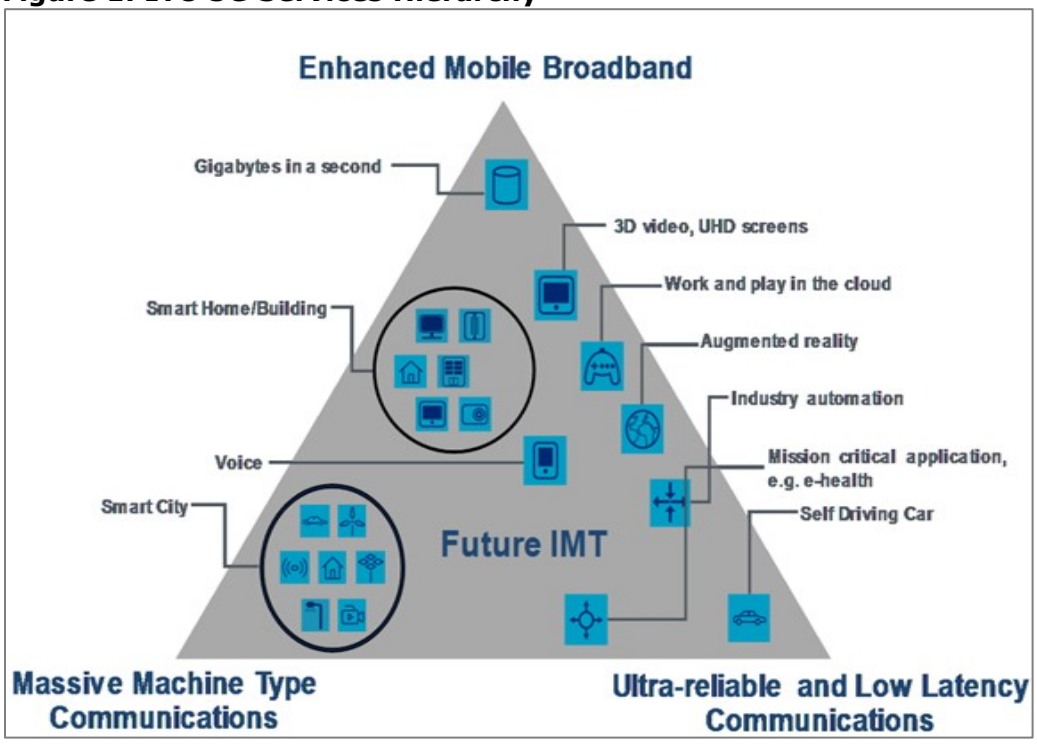
5G is targeting superior performance, including 1 ms latency and 10 Gbit/s peak data rates, both of which represent a quantum leap from 4G networks. These ambitious performance goals have implications on the security performance evolution in 5G networks.

Compared to all previous generations, 5G is the first mobile architecture designed to support multiple diverse use cases. To provide a structure around how the specific domains and accompanying use cases are structured, the International Telecommunication Union (ITU) published the 5G Services Hierarchy.

As shown in **Figure 1**, the hierarchy breaks 5G services into three specific domains. These are the traditional enhanced mobile broadband (eMBB) domain and two new domains: massive machine-type communications (mMTC) and ultra-reliable and low latency communications (URLLC). Each domain has its own unique security requirements. The difficulty of securing such a wide variety of access and service demands via a single integrated 5G network is understandable.

For example, 5G will enable large-scale IoT applications such as the traffic sensors and vehicle-to-infrastructure (V2I) services that are the foundation for smart cities. It is critical that hackers cannot access that data, hijack IoT devices, or disrupt services.

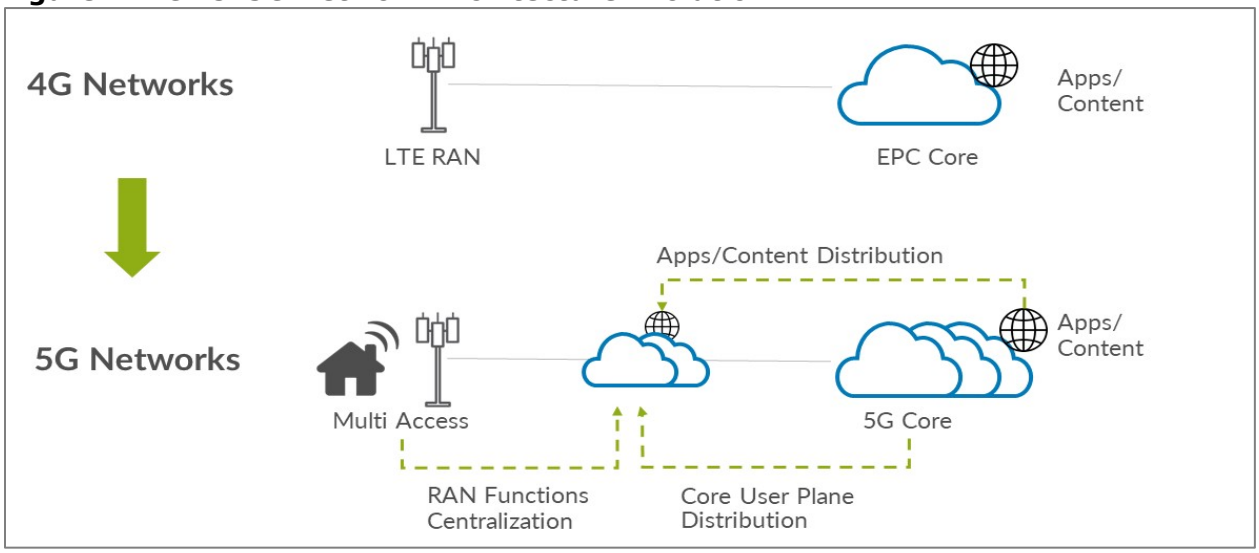
Figure 1: ITU 5G Services Hierarchy



Source: ITU-R M.2083-0

To achieve these divergent performance metrics, 5G incorporates several new network design approaches, including MEC, separation of control and user (CUPS), and network slicing. With this change in network architecture, as shown in **Figure 2**, the security architecture must evolve accordingly. The introduction of new technologies adds new attack surfaces that security strategies must address. These potential risk scenarios are considered in the next section of this white paper.

Figure 2: 4G vs. 5G Network Architecture Evolution



Source: Interpretation of Figure from 5G Americas, The Evolution of Security in 5G

STRATEGY CONSIDERATION #1: SECURITY PERFORMANCE AND SECURITY OPERATIONS MUST SCALE

Like 4G, 5G is not going to be a flash cut. Instead, 5G will evolve side by side with 4G, with logical evolution phases taking place over the next decade. Thus, 4G will continue to remain relevant for many years to come.

As a proof point, GSMA forecasts that 4G will still account for 59% of global connections by 2025.[*] Most 5G deployments will start with the 5G non-standalone (NSA) architecture, which pairs the 5G RAN with the existing 4G core for faster launch of 5G services.

Consequently, service providers' 5G security strategies must first assess existing 4G network security to ensure implementation consistency among both 4G and 5G. The logical starting point to commence this assessment is determining if their 4G network security performance is ready for the increase in network capacity from 5G NSA. In most cases, security will require upgrades to physical infrastructure to scale up and virtual infrastructure to both scale up and scale out.

Without this investment in additional performance, security will become a bottleneck to overall network performance. On a product level, security performance such as throughput, connection scale, and session establishment rate should be evaluated for current mobile security use cases such as 3G/4G Gi/SGi firewall, security gateway (SEG), and Gp/S8 roaming firewall.

Another use case that needs to be examined is distributed denial-of-service (DDoS) protection. With the rise of IoT, connected devices are rapidly becoming a preferred target of hackers due to their massive scale and generally limited security capabilities.

For instance, in 2016, the Mirai IoT botnet compromised nearly 100,000 connected devices globally. These devices launched a DDoS attack against domain name system (DNS) service provider Dyn with a peak capacity of 1.2 terabits per second (Tbit/s), causing more than 4 hours of service disruption and downtime. Mirai was just the beginning. Since then, variants such as JenX, Hajime, Satori, and Reaper have appeared, growing increasingly sophisticated and harder to defend against.

Unfortunately, 5G adoption will only compound the problem by increasing available bandwidth, providing an even more robust network for generating attack traffic from compromised connected devices. As volumetric DDoS attacks grow in terms of frequency, magnitude, and sophistication, traditional defenses such as out-of-band scrubbing centers and manual interventions have become inadequate and cost-prohibitive.

In the case of large volumetric attacks, redirecting suspicious traffic to a scrubbing center adds latency and imposes a significant financial burden, since mitigation costs are directly tied to the volume of the data traffic. Service providers should consider adopting new modern DDoS protection approaches that incorporate telemetry, machine analysis, and network-based mitigation to automate a more intelligent and cost efficient detection and mitigation process.

---

[*] GSM Association, *The Mobile Economy 2019*.

In addition to performance, security operations must also scale and support a distributed telco cloud environment with physical network functions (PNFs) and virtual network functions (VNFs). This requires a unified security management system that manages both physical and virtual domains and provides a unified view of these domains. In other words, security management needs to provide holistic system-wide visibility. Another component of this strategy is to leverage automated policy orchestration through programmable security policies to ensure a reliable and secure network that fulfills service-level agreements.

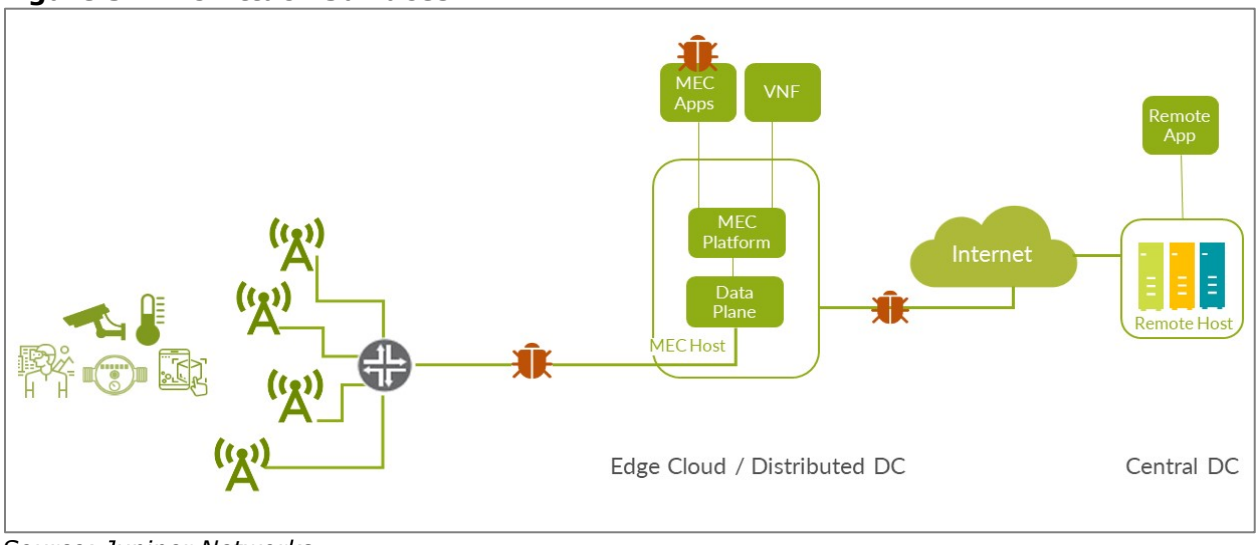
Moreover, 5G infrastructure heterogeneity and complexity will require security to be applied at multiple levels (e.g., associated with a slice, a service, or a resource) across multiple domains. Therefore, security automation and orchestration are critical for service providers to keep ahead of the security operations challenges.

STRATEGY CONSIDERATION#2: NETWORK ARCHITECTURE EVOLUTION AND NEW ENABLING TECHNOLOGIES OPEN NEW ATTACK SURFACES

Edge computing is an evolution of cloud computing that enables application hosting and data processing to move from centralized data centers to the network edge, closer to mobile applications. Edge computing is a key pillar for meeting the demanding requirements of 5G, particularly for use cases where low latency and bandwidth efficiency are critical.

ETSI's Industry Specification Group (ISG) for multi-access edge computing (MEC) has defined a set of technical standards for MEC. These support multiple diverse technologies, including 5G NSA, distributed computing, and the virtualization of networking equipment and computing servers. All of these technologies interoperate in an open ecosystem where service providers can deploy distributed applications. Unfortunately, the heterogeneity and diversity of the MEC environment, as shown in **Figure 3**, introduce a variety of new vectors for malicious attacks and privacy compromises that could constitute a major threat to the entire MEC system.

Figure 3: MEC Attack Surfaces



Source: Juniper Networks

A likely deployment model is to run MEC applications on the same physical platforms as some VNFs. These MEC applications may be third-party applications not controlled by the mobile service provider, which raises the concern that these applications may exhaust resources needed by the network functions.

There are also risks that poorly designed applications could offer hackers an attack vector to infiltrate the distributed data center and affect the network functions running on the platform. Similarly, attackers could insert malicious applications to achieve the same means. If sensitive security assets are compromised at virtualized functions at the edge, an attacker could maliciously reuse them to gain connectivity or carry out spoofing, eavesdropping, or data manipulation attacks.

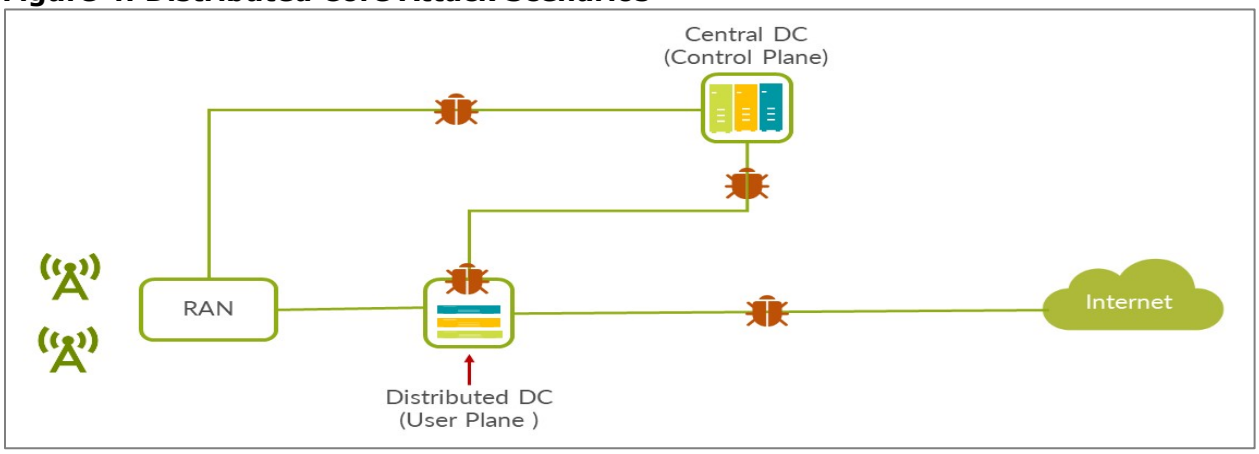
These attack methods are not necessarily new. But since the MEC architecture is new, the potential and gravity of security issues may not be well understood. Therefore, when selecting vendors and before rolling out commercial large-scale edge cloud deployment, service providers should ensure security solutions are flexible enough to meet a broad range of threat vectors at the time of initial deployment.

Distributed Core Attack Surfaces

The introduction of CUPS in the 4G evolved packet core (EPC) represents an important step toward evolution to a 5G core architecture. CUPS is part of the 3GPP Release 14 standard because of its ability to distribute user plane resources across the network with the existing 4G EPC. It can do so prior to the eventual adoption of the new services-based architecture of the 5G core network. CUPS allows operators to locate and scale the control plane and user plane resources of the EPC nodes independently. This works well for high bandwidth applications like video. Because the core user plane is located closer to the end user, operators do not have to backhaul traffic all the way to central data center. Therefore, they can reduce latency and backhaul costs.

While CUPS is not a 5G feature per se, it conforms to the new trust boundaries and threat surfaces inherent with 5G network deployments. This means, as shown in **Figure 4**, that any interface including Sx and SGi can be targeted to enable the launch of DoS or DDoS attacks.

Figure 4: Distributed Core Attack Scenarios



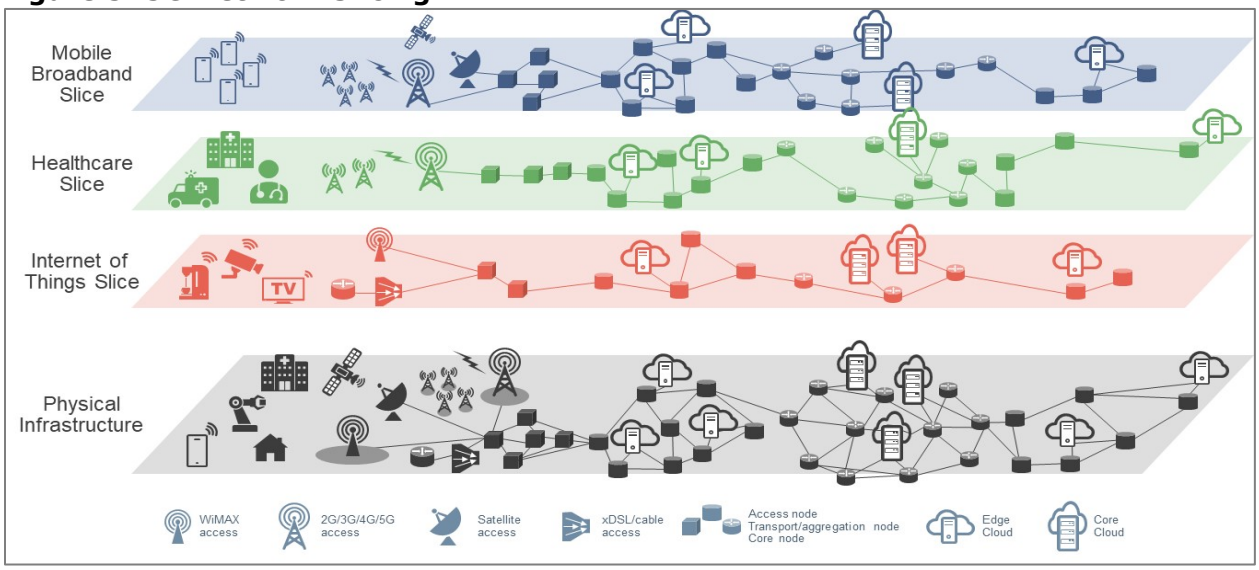
Source: Juniper Networks

Network Slicing Attack Surfaces

Network slicing is a specific form of virtualization that allows multiple logical networks to run on top of shared physical network infrastructure. With network slicing, mobile service providers can partition their network resources to address a diverse set of use cases with different performance and functional requirements from very different users. They can also multiplex these use cases over a single physical infrastructure.

For example, as shown in **Figure 5**, it is now possible to create distinct application slice types to support a broad range of services, including industrial IoT and healthcare vertical-specific applications.

Figure 5: 5G Network Slicing



Source: IEEE, Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges

Network slicing is expected to play a critical role in 5G networks because of the multitude of use cases and new services 5G will support. These new use cases and services will place different requirements on the network in terms of functionality. The performance requirements may vary significantly in terms of throughput, quality of service, latency, and security, as indicated in the ITU 5G Services Hierarchy (see **Figure 1**).

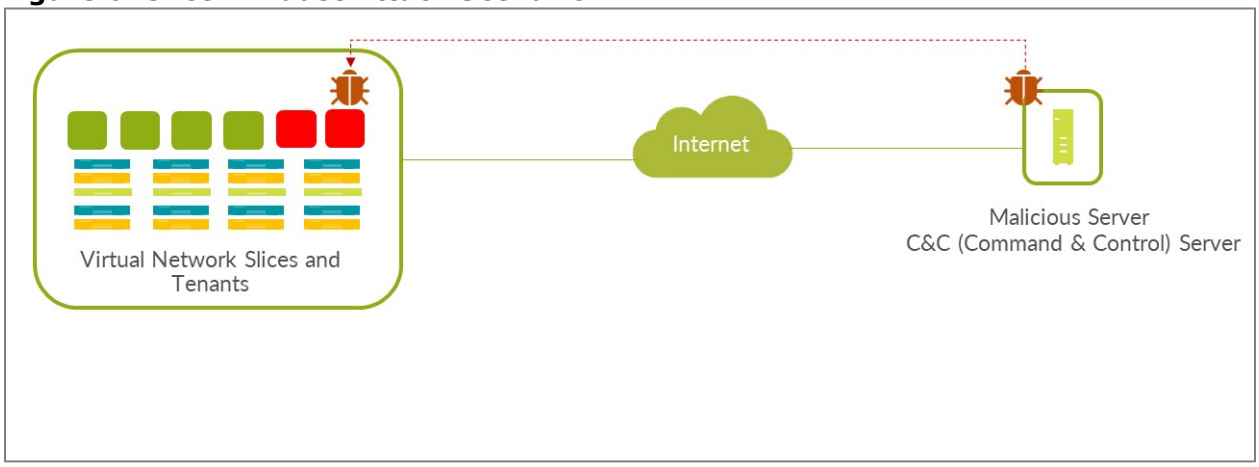
One commonly cited example in 5G is the sharing of a given physical network to simultaneously run massive IoT, mobile broadband (MBB), and URLLC applications. For example, IoT will typically support a very large number of devices, but each device may have very low throughput. In contrast, MBB will support a much smaller number of devices, but each one will be transmitting or receiving very high bandwidth content.

These varying service slice performance profiles have a direct impact on security protocol choices and policy implementation. For instance, the service in one slice may require extremely long device battery life, which constrains the security protocol in some other way (e.g., how often re-authentication is performed). In another example, the service in one slice may be very privacy-sensitive, requiring unusually intensive security procedures (e.g., very frequent reallocation of temporary identities).

Furthermore, service providers need to consider how well these slices are isolated from each other. One of the main security concerns involves bad actors gaining broader network access via a "lower" security slice.

As shown in **Figure 6**, an attack scenario could involve an attacker that exhausts resources in one slice. In doing so, an attacker may exhaust resources common to multiple slices and hence cause DoS or service degradation in other slices, too.

Figure 6: Slice Exhaust Attack Scenario



Source: Juniper Networks

STRATEGY CONSIDERATION #3: SECURITY AS A REVENUE DIFFERENTIATOR AND ENABLER

A final consideration for service providers' 5G security strategies is how to leverage security to differentiate and monetize their network deployments.

The adoption of 5G capabilities such as network slicing will facilitate strong revenue growth across many segments, including the manufacturing and transportation sectors, which will rely heavily on IoT applications. Unlike consumers, many of these industry verticals have more stringent requirements of security. Therefore, historically, many have built their own private networks for connectivity. To successfully penetrate these vertical markets with 5G offerings, service providers should highlight their security capabilities for serving these customers' needs and addressing their concerns.

In the context of IoT, service providers have an effective entry into the enterprise IoT conversation: connectivity. While the potential in IoT connectivity is sizable in itself, service providers can capitalize on many other opportunities. For example, security. Security remains a top concern and technical barrier for enterprises to adopt IoT.

Since many companies in these sectors will likely not have the internal skill sets to secure their applications, they will turn to service providers to assist them with their unique security requirements. This is an important step that permits service providers to move beyond providing basic connectivity services and evolve to deliver IoT connectivity and security into compelling offerings.

Another area where security can be positioned as a revenue enabler is 5G security as a service (SECaaS). Much of the attractiveness of 5G lies in enabling vertical industries to improve cost/efficiency by using shared infrastructure. Some verticals may wish to remain in control of security while others may opt for further savings by outsourcing selected security services to the 5G network. These services could include placing policy enforcement (firewalls, device access control) in the network and/or relying on authentication/ geolocation assertions provided by the network.

Software-defined networking and virtualization technologies enable the deployment of security configurations for specific applications or users. By isolating application-specific connections from each other, 5G service providers can offer to provide customized per-user security capabilities such as monitoring analytics and deep packet inspection as value-add services.

Similarly, for scenarios where service providers host third-party applications in their MEC/ edge cloud environment, there is an opportunity to offer security/assurance services for those applications. Some service examples might include performing integrity assurance checks on applications at installation and during upgrades and server restarts. Another example could be exposing security service APIs to sufficiently trusted third-party MEC applications for user identification.

CONCLUSION

Security is an essential component of successful 5G service delivery. Service providers must ensure their security strategy is well planned as an integral part of 5G evolution roadmap.

Current mobile network security performance and operations must be able to scale up and scale out to meet 5G requirements instead of being a bottleneck. Furthermore, since edge computing, CUPS/distributed core, and network slicing introduce new attack surfaces, service providers must implement proper security measures capable of mitigating threats. Finally, security in the 5G and IoT era should not be considered just a liability. Instead, service providers should consider positioning security as a key service differentiator and essential revenue enabler.