# 5G SECURITY

## Establishing a Holistic Approach to Paving the 5G Evolution

# Table of Contents


5G: The Journey 3

Differentiators to 5G Adoption 3

Debunking 5G Security Myths 4

What's Different About 5G With Regard to Security? 4

Risks and Implications for Service Providers 5

Security in 5G Requires a New Approach 5

Conclusion 6

### 5G: The Journey

Mobile network operators, or MNOs, have embarked upon their "next evolution": a journey to build out 5G networks that will enable an unprecedented number of mobile services at greater speeds, and across billions of devices and things. This will unleash such new services as high-definition video, self-driving cars, massive adoption of the internet of things (IoT), smart cities, and a mass digitization of businesses and industries.

5G promises transformative mobility by offering enhanced mobile broadband experience and enabling industrial digitalization through customer value creation. Mobile network operators will have the opportunity to utilize their networks to enable new business models tied to enterprise business services. Operator revenues are predicted to grow at a CAGR of 2.5 percent to reach $1.3 trillion in 5G services by 2025.

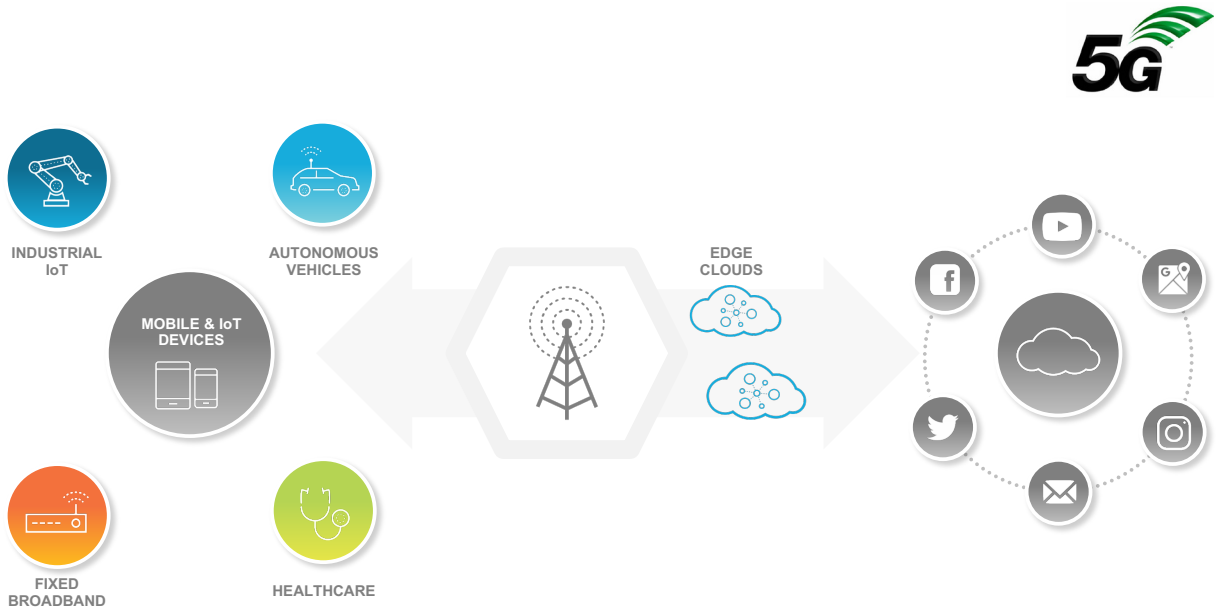


**Figure 1:** 5G industrial digitization

5G networks will evolve in multiple stages over the next decade. Applications and services that were traditionally consumed as over-the-top, or OTT, services required best effort connectivity. With 5G, use cases for life-critical and business-critical services catering to key enterprise verticals will have more definite requirements on connectivity, security and targeted SLAs. Securing 5G becomes critical, giving a chance for operators to move up in the value chain from being only connectivity providers to secure business enablers.

### Differentiators to 5G Adoption

It's also clearly understood that security is a fundamental enabler for 5G. Naturally, a great deal of emphasis in these early stages of the 5G evolution is being placed around delivering the higher data speeds, the latency improvements, and the overall functional redesign of mobile networks to enable greater agility, efficiency and openness.

*Device-Initiated Threats Are Real*

Tier 1 service provider suffered massive outage after Mirai compromised 900,000 routers

Casino hacked through internet-connected fish tank thermometer

**Figure 2:** Notable device-initiated attacks

While the new types and classes of applications will offer new revenue opportunities for the operators, the explosion of low cost, low power and unsecured IoT/sensors using NarrowBand IoT will also pose expanded security risks for the operator's network and end users.

Establishing the right security approach across 5G networks is critical and requires consideration of some new requirements and challenges, while recognizing there are a few myths that need to be debunked. The basic questions covered here include:

- What is different about 5G with regard to security?
- What are the new risks and implications for service providers?
- What is the right 5G security approach to establish and how will this evolution take place?

## Debunking 5G Security Myths

To help address these fundamental questions, let's first debunk a few common myths associated with 5G security.

### *Myth #1: As 5G Networks Evolve, All You Need to Do Is Make Existing Security Elements Perform at Faster Speeds*

The rapidly evolving threat landscape has tremendous security implications on the 5G networks impacting consumers, businesses and the operator's own mobile network. Service providers have reached an inflection point where they must take an entirely different approach with security. A Layer 3/Layer 4-based security approach is simply not positioned to handle the sophisticated challenges of today and tomorrow effectively. Establishing a strong security framework is much more than just stitching together ad hoc security modules in an attempt to offer 5G security. Disconnected security modules will not scale, and security cannot be applied consistently throughout the network. A hop-by-hop security mechanism is not enough to build the differentiated end-to-end security that 5G demands. A holistic and completely new approach to security is needed.

### *Myth #2: CGNAT Provides Security at the Internet Edge*

Critical mobile network infrastructure is often left unprotected based on the assumption that a CGNAT device offers protection for subscribers and devices by IP translation mechanisms. In reality, CGNAT as an inline device offers very little protection to IPv4 devices and traffic, and does not offer any protection for IPv6 devices and hosts. In addition, these network devices maintain huge volumes of state information, making them vulnerable and often subject to DDoS attacks from the internet. CGNAT devices can be the first points of failure during these attacks. Hence, CGNAT needs to be augmented with a firewall.

### *Myth #3: 5G Is Here – So Investment in 4G Security Can Be Capped*

5G is not going to be a "flash cut" of networks from 4G to 5G. 5G will evolve side by side with 4G, with logical stages of evolution likely taking place over the next decade before we get to a critical mass of 5G subscribers. GSMA forecasts, by 2025, 4G will still account for 66 percent of global mobile users. Early 5G deployments will be brownfield, made possible by 5G non-stand-alone architectures leveraging existing 4G core for faster launch of 5G services, while operators start rolling out 5G stand-alone architectures for greenfield deployments. 5G security approach must start with existing 4G networks, and should be addressed consistently across 5G.

## What's Different About 5G With Regard to Security?

A major business driver for the evolution to 5G networks revolves around enabling business-led transformation with more open mobile networks that leverage a service-based architecture, or SBA. 5G networks will undergo a fundamental shift in architectures from today's mobile network architectures. A key aspect of this shift will include applications and services moving out to the mobile edge and enterprise services being provisioned and hosted on these networks. Massive IoT, smart utilities and smart cities, in particular, are seen to be among the first transformative industry applications of 5G, according to NGMN.

To make this 5G vision possible, a significant evolution from today's mobile network architectures will take place over time that will open up new security vulnerabilities and threat vectors, taking into consideration the approaches that follow.

### *Threat Vector Proliferation*

Threats do not wait for 5G. Large-scale attacks can come from anywhere, even from within the operator's own network, through a botnet comprising tens of thousands of large-scale, weaponized IoT devices. 5G radio network deployments include significant expansion of small cells connecting over untrusted networks, greater use of cloud RAN, 5G-NR across unlicensed spectrum, device-to-device communications, and devices connecting to multiple cells. This evolution further intensifies the impact on the security landscape with growth in the number of potential intrusion points. IoT infected with malware can produce huge signaling storms impacting the evolved packet core, or EPC, resulting in outages or service degradations. Deep visibility and control across all layers, including application, signaling and data, at all locations is required.

### *Applications and Services Move to the Edge*

Traditionally, operators have been just a connectivity provider with applications, and services were delivered as over-the-top, or OTT services, from the service provider data center or on a Gi interface from the internet. With 5G serving business-critical and life-critical use cases for key industry verticals, edge computing technologies are being deployed to support low latency requirements, enabled by multi-access edge computing, or MEC. This introduces a highly distributed computing environment, requiring the need for effective security at the edge. MEC plays a key role in accelerating network transformation vision in 5G and also enables the operator to move up in the value chain to become a secure business enabler.

### *Network Slicing and Software-Driven Agility*

5G mobile networks will support verticalization of services across industries and are expected to be built in a way to enable logical network slices to allow operators to provide networks on an as-a-service basis to meet the wide range of 5G use cases. These slices will require different service levels, strong isolation per slice to prevent threat propagation, and security policies instantiated per slice.

Technology shifts to software-based approaches like SDN and NFV will bring agility and flexibility through network modernization, shortening the time to bring new services to market and enabling rapid service deployment. However, these approaches introduce complexity in the network. A cloud-ready NFV platform that supports open APIs and offers consistent security across software and hardware is required to enable the distributed architectures that 5G brings.

## Risks and Implications for Service Providers

Security in 5G must be tightly coupled with business services. Mobile operators can leverage 5G hosting centers to host enterprise applications for industry verticals. Industries rely on the operators to serve their applications, and security is viewed as a shared responsibility for operators and businesses.

In a survey conducted by Ericsson,[1] which included Top 20 global mobile service providers, 90 percent of respondents identified security as a key differentiator in 5G adoption.

5G security vulnerability fuels operators' business risks to offer reliable and secure availability of life-critical consumer applications and business-critical enterprise mobile services. Establishing a high reputation index will be critical for mobile network operators to build profitable 5G business models.

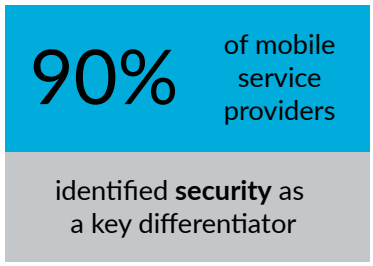


**Figure 3:** Key Ericsson finding about security

## Security in 5G Requires a New Approach

With the scope of 5G services expanding, as we've noted, dealing with the evolving security challenges and risk factors requires a holistic and transformative security approach across the mobile networks so you can:

- **Adopt a preventive approach to security.** Application/Layer 7 visibility and control across all layers, including application, signaling and data, at all locations is required. Reduce the attack surface, find anomalies and malformed traffic to become much more equipped to proactively handle the threats on the RAN and roaming interfaces.
- **Increase levels of security automation.** Both 4G and 5G networks are becoming more open, more virtualized and more distributed. Effective 5G security outcomes will require actionable insights at cloud scale. Cloud-based threat prevention, powered by advanced big data analytics and machine learning techniques, is critical to provide swift response to known and unknown threats in real time.
- **Establish contextual security outcomes.** Data-driven threat prevention provides contextual security outcomes. Leverage GTP visibility and threat intelligence, and correlate the threat to the attack source, to find and isolate infected devices before botnet attacks can potentially take place.
- **Integrate security functions with open APIs.** A single pass-platform with open APIs provides operational simplicity with NFV/SDN architectures. As 4G/5G networks evolve, more functions will become virtualized and deployed in telco cloud environments. Advanced network security efficacy being put in place with 4G needs to seamlessly evolve with the networks. Cloud-ready NFV supporting open APIs offering consistent security across software and hardware is required to support the distributed architectures that 5G brings.

1. "Exploring IoT Strategies," Ericsson, April 2018, https://www.ericsson.com/en/internet-of-things/trending/exploring-iot-strategies.

## Conclusion

As 5G begins to roll out, organizations are increasingly looking to service providers for a resilient network with robust security mechanisms in place to secure their connected customers, and make sure applications and services that come across their networks are clean and secure. Prevention becomes more critical than ever. Establishing application-layer visibility and consistent security all locations across the mobile network is essential to providing future-proof security.

Some key outcomes from establishing the right security approach will carry forward to 5G and assure:

- Consistent security across the entire 5G network architecture – within the core network and distributed out to the edge.
- A clean 5G network that prevents malware from transporting across to connected devices and protects customers from cyberattacks.
- A 5G network with security mechanisms that prevent unauthorized command and control, aka C2, from exploited connected devices.
- An open and secure 5G network that enables network resources to be securely exposed to third parties – so mobile operators can maximize 5G adoption and monetization of 5G network resources.
- A 5G network with automated threat hunting mechanisms in place across key points in the core network and out at the edge – allowing for quick identification of infected hosts and rapid resolution of security-related incidents.
- A 5G network with prevention mechanisms in place, which keeps malware from getting onto network functions that can then spread across other functions and infect individual 5G slices.

Service providers are in a position to capture the economic benefits that 5G brings and enable high-value mobile networks for a secure 5G digital economy. Become massive technology enablers and trustworthy partners for your customers by building differentiated networks to maximize the business opportunity and minimize liability risks.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com


5G-security-wp-110918