# A Comprehensive Approach to Securing 5G Networks and Data
**September 2020**

***Summary: Managing the security of telecom networks and the data that runs on them is a challenge, particularly in the context of the evolution to 5G. Due to its compelling value proposition as a major driver of business transformation, 5G adoption is growing rapidly across numerous industry verticals worldwide—bringing a new threat landscape. When it comes to 5G cybersecurity, some stakeholders focus on the trustworthiness or security of particular technologies or vendors in the network and consider excluding them accordingly. While vendor supply chain security is important, this narrow approach does not account for how telecom networks are architected and operate, nor the full picture of cybersecurity threats and risks to networks and end-users. As a result, this approach does not enable effective management of all risks. This paper explains how telecom networks have evolved and concludes by describing proven, state-of-the-art security tools and capabilities that operators can use to manage today's cybersecurity risks and secure their networks and data regardless of underlying technology or vendor.***

## ❖ The architecture of today's telecom networks: Multiple technologies and vendors

Telecom networks have undergone a large technological shift. Networks leverage more types of technologies than ever before, which has radically changed the necessary approach to security.

Traditionally, networks were largely composed of physical equipment, such as hardware switches (devices that enable communication between devices) and routers (devices that select paths for traffic in a network or between or across networks). These were core network elements and IT services hosted on closed and proprietary hardware. Equipment often was placed in operator-controlled physical premises with dedicated communications links.

Today, while physical elements still exist, networks have evolved radically, a transformation that began in the 4G era and is already a model for 5G networks (in fact, telecom networks of the foreseeable future will be a combination of 4G and 5G technologies). Networks are dynamic and scalable, largely software-driven, virtualized, and decentralized. These changes have been enabled by network function virtualization (NFV)[1] and software-defined networking (SDN)[2] technologies. Telecom networks are also now cloud-ready, and many operators prefer a multi-cloud strategy as the better operational model, often procuring from multiple vendors.

[1] NFV is the decoupling of network functions from proprietary hardware appliances and running them as software in virtual machines (VMs).
[2] SDN is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.

Operators seek to rely on end-to-end automation for network operations and service delivery. All these physical and virtual technologies combined make up modern telecom networks.

Whether rendered in hardware or software, a telecom network is split into 'core' networks and 'access' (or edge) networks.[3] In 3G and 4G networks most computing power and processing/ service delivery emanated from the core. For 5G, the core network is expected to be highly distributed and access will be complemented by mobile/multi-access edge computing (MEC).[4]

- The "core" or data center. The network's central element, the core acts as a hub for all the data traffic and all the user metadata needed to give a user service. Ultimately, the 'core' ensures data goes to the right place. The core can be dedicated hardware or a software-based data center in a public (shared) cloud or a telecom operator's exclusive private cloud. The core could be centralized or geographically dispersed.
- The 'access' network or edge. This manages the user's local access into the network and routes their data traffic towards the core. Access networks are located closest to end users such as businesses, customers, or individuals and consist of small devices or access points (e.g., base stations, antennas) which provide entry points into core networks. Access networks can physically exist or be virtualized/ cloud-based.

Parallel to this technological change, telecom networks now rely on multiple diverse vendors than ever before. No single vendor can provide all the types of hardware, software, and services that telecom networks need to operate. Instead, today's telecom networks must "mix and match" multiple vendors from across the globe producing various technologies that must be integrated seamlessly. Examples of technologies in today's 4G/5G telecom networks include diverse hardware such as networking and storage; software to enable business service functions like fulfillment, service assurance, and operations support; and cloud technologies. A range of vendors provide these technologies and more.

There are many benefits of these modernized, cloud/software-driven telecom networks. These networks have lowered operators' business costs. The networks are agile, flexible and can meet performance and scalability requirements (particularly of diverse 5G-enabled service offerings), offering on-demand provisioning of bandwidth or services. They enable rapid deployment of new services, shortening time-to-market and helping operators stay competitive.

### ❖ The evolving cybersecurity challenges facing today's telecom networks

Cybersecurity challenges facing today's telecom networks are twofold.

- Challenges due to architectural shifts. The massive increase in network connectivity, move to software-driven networks, and emergence of new types of applications pose expanded

[3]The core is also termed "evolved packet core" (EPC). The "edge" is often referred to as the "radio access network" (RAN). Private enterprises that build their own private 5G networks use this architecture as well.
[4]MEC moves the computing of traffic and services from a centralized cloud to the edge of the network.

security risks for both telecom operators and their end-users/customers. The shift towards virtualization also requires new security practices. While software-driven models help drive agility, they make networks more vulnerable to attacks introduced by the software platform and underlying operating systems, including host vulnerabilities, linux threats, and hypervisor/ container vulnerabilities. Networks can be vulnerable to lateral threat movement across virtual network functions, cloud-native functions, and business and subscriber service functions. Further, the merging of 5G with 4G means that the 5G networks inherit the risks and vulnerabilities from 4G. Finally, risks are no longer confined to the data center; the whole landscape is becoming more distributed, and hackers are targeting devices outside traditional perimeters. In fact, the traditional perimeters will no longer exist in 5G networks.

- Evolving cyberthreats and cyberattacks. At the same time, cyberattacks on network infrastructure and users continue to grow in volume and sophistication. Adversaries consistently introduce and update new attack tools, utilize automation, and leverage the cloud to attack network infrastructure, applications, services, and operators' customers/ end-users (enterprises). Threats traversing networks include command and control (C2), malware, and viruses. Threats are amplified in 5G, where attacks leverage 5G speeds and there are many new points of attack as IoT devices proliferate. All of this makes securing networks, data, and end devices even more critical with the advent of 5G.

### ❖ Today's challenges require a different approach to telecom network security

Everything described above means we must revisit the conventional approach to the security of telecom networks, especially as they become increasingly virtualized. In the past, security was provided by physical protection and isolation of traditional telecom network systems, relying on perimeter security. With decentralization, this is no longer useful or effective. Now, any quality issues or flaws in a product (such as poor software development/ coding or vulnerability management, poor system patching, or vulnerable hardware) can impact the broader network. Such flaws could potentially result in widespread disruption to operations or be exploited by an attacker to gain control of network equipment and data via backdoor communications.

There are three overall characteristics of how telecom networks must be secured.

- **Shared responsibility.** While individual ICT vendors remain responsible for securing their own proprietary hardware, software, or unique offerings deployed in a network, telecom operators have the ability to secure the network infrastructure and communications/ data traversing networks.[5]

[5] Of course, consumers of 5G services who own the data, applications, and devices and the enterprise users operating on 5G networks also must manage their risks when using 5G networks. They must have visibility, control and ultimate authority into which users and devices have a legitimate need to access specific applications and data using the 5G network. Enterprise users can exercise this responsibility directly or via enterprise services provided for their control via their 5G provider.

- **Securing device and communications traffic.** Because all telecom network elements need to communicate to perform the various functions and provide the services the telecom operator seeks to provide, security of the device and communications traffic is imperative. Real-time visibility and enforcement of threats traversing the networks, supported by a Zero Trust approach, are essential. Under the Zero Trust model, everything and everyone trying to connect to the network, or data traversing the network, should be verified before access is granted—this requires network segmentation and granular enforcement.
- **Automation.** Security policies, detection and mitigation should be automated with the cloud-based threat analytics and behavior analyses powered by artificial intelligence (AI) and machine learning (ML) techniques.

❖ **Proven, state-of-the-art, scalable security tools and capabilities exist**

Security tools and capabilities are available to operators to secure today's complex network infrastructures, communications, and data, regardless of underlying technology or vendor in the network. These tools and capabilities can overlay a telecom infrastructure and serve to secure all traffic traversing the network infrastructure, services, and applications. Important functionalities of these security tools and capabilities are described below.

- ***Maintaining constant real-time visibility and enforcement.*** Telecom operators need to have constant real-time visibility and enforcement of traffic interactions between and among diverse network elements as well as into and out of the network itself and be able to detect and stop in real time cybersecurity threats within that traffic. For example they can leverage mobile tunnel[6] traffic inspection for automated visibility and enforcement of security threats and attacks to determine whether traffic flowing in their networks is malicious or benign and respond accordingly.[7] The ability to leverage visibility to correlate malware and vulnerabilities to the source / destination of threats is critical to protect networks, services, and businesses.

- ***Leveraging real-time mitigation.*** This is critical in responding to correlated threats and to taking actions—for example, dynamically isolating infected subscribers and devices before botnet attacks can potentially take place and offering actionable insights for faster security troubleshooting.

- ***Authenticating that devices and users are who they claim to be*** before they can perform a certain action, such as requesting data. Not all devices/ users require access to all resources. For example, a mobile subscriber traversing the infrastructure, or an IoT device

[6] A "tunnel" is a temporary virtual connection established to send data/traffic from point A to point B.
[7] The GSMA issued recommendations for MNOs to detect and prevent attacks within GTP-U tunnels, titled "FS.37 - GTP-U Security" https://www.gsma.com/security/resources/fs-37-gtp-u-security/ (March 2020). The GSMA is an industry association representing the interests of mobile operators worldwide, including more than 750 operators and almost 400 companies in the broader mobile ecosystem.

connected to the network, must be verified as a legitimate user of the network and not a hacker who has tampered with or spoofed a physical device or SIM card.

- ***Controlling the level of access each device or user is granted*** to certain resources, based on sensitivity or criticality. This is important both laterally (within networks), and into/out of networks. For example, telecom data centers hold sensitive data, such as customer databases with billing records and personal information, that only authenticated users should access.

- ***Internally dividing/segregating network elements,*** based on level of risk (between sensitive and non-sensitive data, or high-risk elements) or function, and managing communications between disparate elements accordingly. This can ensure that network elements act only according to their defined role and do not have unauthorized interaction or communication with other parts of the network or outside the network (e.g., trying to connect to an unauthorized external C2 server in order to pass sensitive data). Further, if one part of a network is impacted by a threat, the threat cannot move to another part.

- ***Securing the "containers" used to build the 5G core.*** Software updates to virtual machines traditionally have required upgrading the whole machine with a new software release, an approach that brings significant risk due to software complexity and interdependencies. Containerization, which is widely used to build the 5G core, breaks code into small portions with defined infrastructures; code can be updated by removing and replacing an individual container, allowing for dynamic, continuous, less-risky change. Containerization can automatically check code as it is being written, scan it while it is being deployed into the infrastructure, and ensure the code can talk only to relevant parts of the infrastructure. As container adoption rises, so should the adoption of best practices for container security to protect running containers in production as well as secure containers across the full application lifecycle. This should be complemented by secure agile software release practices based on continuous integration and continuous delivery/deployment (the CI/CD pipeline). The CI/CD pipelines that scan for host and application vulnerabilities provide a head start on securing the container compute infrastructure.

In all the above, it is imperative to prioritize prevention, automation, and orchestration. Preventing threats is crucial: While response to and recovery from incidents are important, at that stage damage is done. Automation is vital against increasingly automated and sophisticated attackers and must replace manual response, which is time-consuming and costly and cannot scale against automated attacks. Security orchestration provides workflow automation and oversight across security products to address challenges faced by security teams who struggle to execute standard processes across products in the face of rising incident alert volumes.

## ❖ Conclusion

Governments and industry share the goals of mitigating cybersecurity threats to telecom networks and data, preventing successful cyberattacks, and reducing the impact of related cybercrime. As in all areas of cybersecurity, achieving these goals is a shared responsibility, and governments and industry should collectively develop plans that will ensure that our critical lifeline activities enabled by 5G deployments are appropriately secure. While excluding vendors or technologies may seem to some like an appropriate response, doing so will not mitigate all cybersecurity risks or vulnerabilities. Threats will still traverse the networks, and hostile actors will work to access sensitive data or exploit vulnerabilities in hardware or software deployed in a network.

As government policymakers seek to address concerns about cybersecurity in 5G networks, they should:

- ***Encourage the use of state-of-the-art, scalable security tools and capabilities*** that can secure modern telecom networks, communications, and data regardless of the underlying technology or ICT vendor in the network.
- ***Promote and incentivize ICT vendor best practices and transparency,*** ranging from controlled product lifecycle and security management to security testing to vulnerability and issue management.
- ***Work with vendors that are open to shared responsibility and demonstrate best practices*** and avoid those that are not willing to adopt this open approach.
- ***Promote automated sharing of actionable cybersecurity threat information*** among operators and other stakeholders for better situational awareness and prevention of successful cyberattacks.