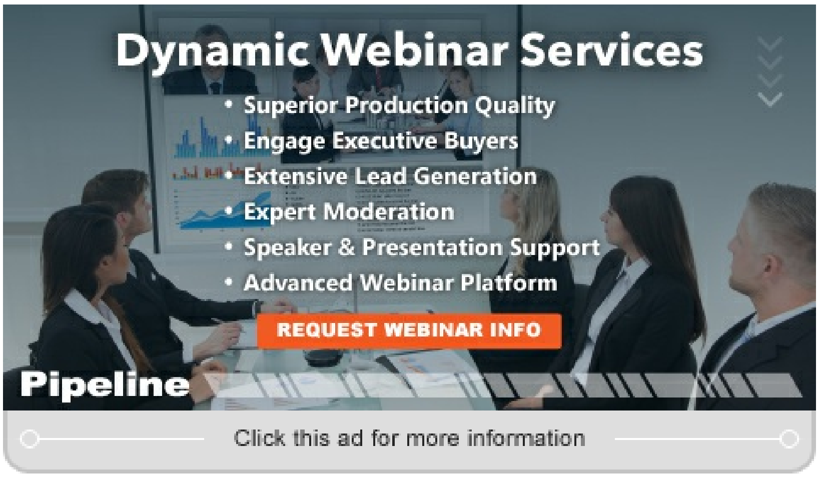
Designing for Security in 5G Networks

By: Mary O'Neill

Communications Service Providers (CSPs) and consumers expect great things from 5G. Yet disruptive technologies such as 5G, the Internet of Things (IoT) and the cloud are quickly changing the technology landscape and are creating many potential cyber-risks for malicious attacks. Cybersecurity statistics reveal a huge increase in hacked and breached data from sources that are increasingly common in the workplace, like mobile and IoT-connected devices.

In fact, in the first six months of 2019, data breaches exposed 4.1 billion records. With 5G being a complete transformation of the end-to-end network from the radio via the transport to the core, attacks can affect millions of interconnected and vulnerable nodes.

In this era of 5G, consumers and businesses will demand that their data is confidential, privacy is respected, and operations and transactions are secure. New use cases and the adoption of new networking methods demand a different approach to security for 5G on top of standardized and already existing safeguards. This new approach necessitates security operations that are both predictive and automated. Also, CSPs will need to increasingly utilize analytics and machine learning, orchestration and workflows and threat intelligence to ensure rapid and efficient responses to threats.


Dynamic Webinar Services
• Superior Production Quality
• Engage Executive Buyers
• Extensive Lead Generation
• Expert Moderation
• Speaker & Presentation Support
• Advanced Webinar Platform
REQUEST WEBINAR INFO
Pipeline
Click this ad for more information

Many 5G-enabled use cases require inherent security that exceeds existing 3GPP standards and encompasses security automation, orchestration, analytics, and machine learning to detect and mitigate threats. Building this security into 5G networks means treating the entire network as a sensor as well as a shield. Data is now taken from many or even all existing 4G and 5G systems and is used to provide a much greater level of insight than in the past. The triggered responses to threats or security issues are achieved through automated workflows that incorporate business processes. This approach detects an irregularity and then suggests a way to fix it based upon standard playbooks. Today, this is done in the best case by scripting, but this new, extensive 5G security automation frees up the security experts to focus on more immediate or higher-priority threats.

Building trust: a growth opportunity for CSPs

As 5G becomes a reality, CSPs are seeing enormous potential to create new revenue streams by offering innovative and highly anticipated 5G services to new customers and industry segments. However, CSP success depends strongly on their ability to build digital trust to ensure enterprises and end users have the confidence they need that their data and private information are secure on 5G networks.

CSPs can develop higher digital trust by highlighting their full compliance with relevant regulations governing network security and data confidentiality to customers or industries. Recognized requirements already mandate CSPs to comply with lawful intercept, user privacy, and customer notification of security breaches. However, they need to meet several new regulatory requirements. These include industry standards such as the Cyber Security Act, the Payment Card Industry standards, and the EU’s General Data Protection Regulation (GDPR). In the future, a CSP may also be required to show a specific level of security for its 5G infrastructure (e.g. NESAS).

5G demands new approaches

New security concepts are required for the next mobile network generation because 5G supports new use cases and the adoption of new networking methods. The open 5G network of the immediate future will consist of a complex ecosystem of multiple stakeholders. This ecosystem requires trusted and trouble-free interaction.

Not all customers, though, need the same levels of security. For example, an online gamer and a large retailer have quite different security needs. Security measures must therefore match each use case. This is where network slicing comes in. Network slicing, one of the newest technologies enabled by 5G, addresses this issue by allowing different levels of security to be offered to users of different services. In more detail, 5G network slicing is a network architecture that enables the multiplexing of virtualized and independent logical networks on the same physical network infrastructure. Each network slice is an isolated end-to-end network tailored to fulfill diverse requirements needed by a particular application. Isolated network slices also help to confine a cyberattack to a single slice. Because of this, network slicing takes a starring role in supporting 5G mobile networks that are designed to efficiently embrace a wide array of services with very different service-level requirements, including security KPIs.

The new approach to security for this new type of 5G network requires service providers to develop four key capabilities to help them operate all the integral and standalone safeguards to build customer trust. When combined, these capabilities help ensure properly secured—and thus reliable—new 5G services.

Key 5G security capabilities

The four 5G security capabilities necessary are adaptation, speed, integration, and automation.

Adaptation means that a CSP can respond quickly to deal with cyberattackers’ increasingly sophisticated techniques.

Speed is important because it is one of the most important success factors in reducing the length of time a hacker goes undetected. In 2018, the median dwell time in the corporate sector was estimated at 78 days. By being able to increase response speed through analytics, machine learning, and automation, this time can be cut by up to 80 percent.

Integration of as many different security tools and systems as possible into a central reporting system reduces the time needed to filter out false alarms and respond to genuine threats.

Automation reduces the growing workload facing security teams. 5G cybersecurity uses automation to deal with recurring attacks by using pre-defined, automated responses. This security automation translates into more efficient provisioning, security configuration and hardening, and delivers higher quality.

Different 5G network domains = unique security requirements

Security in 5G networks isn’t a one-size-fits-all endeavor. Each domain and technology that makes up a 5G network has its own risks and causes different business impacts. As such, each has varying security priorities.

The wide array of machines or end points that connect to and exchange data with a 5G network expose it to numerous risks. Establishing trust by managing these end points means involving industry best practices like two-way authentication, signed software delivery, certificates, and encryption. Using artificial intelligence (AI) to analyze traffic patterns and detect anomalies should be self-explanatory for critical IoT devices and services.

For 5G radio access and transport security, tunneling data avoids the need to set up individual security for different sessions. Encrypting control and management traffic planes protects traffic and hides the core network to prevent an unauthenticated element from connecting to it. Encrypting the user plan will be demanded by critical or sensitive slice-customers to protect the data from being transmitted.

In the cloud’s shared infrastructure, new security challenges can be dealt with via a number of security measures. Virtual network functions (VNFs) need to be separated, and this can take place with virtual switches, vLANs, and wide-area VPNs. Virtual firewalls also help to provide security.

For 5G core security, dividing the 5G core into security zones helps to control and monitor traffic and enforce the integrity of its data. Confidentiality rules can be set for each zone, making it significantly harder for threats to spread from one domain to another. This will be important, as the core will be highly distributed to support new use cases. It is similarly important that the network functions within the Service-Based-Architecture (SBA) are properly using certificates and TLS as recommended by 3GPP.

5G security with analytics and automation

5G networks cross many discrete infrastructure domains and contain numerous physical and virtual network functions. Thus, security management and efficiency are more challenging than in older networks because of the complexity of the architecture, which includes distributed RAN, cloud RAN, edge core, and cloud core. This complexity requires automated workflows to reduce the time and effort to provision services to meet varied service level agreements (SLAs).

Security, Orchestration, Analytics and Response (SOAR) deals with this complexity by orchestrating and automating responses by executing a playbook to validate whether an event is based on human error or if it is an attack. The key principles of SOAR include:

- Constantly measuring security posture and risk levels
- Controlling and limiting access to key operational systems and assets
- Detecting threats earlier in the mitigation chain
- Rapid response to minimize the impact of cyberattacks

The security team can rely on fast, automated responses with a 5G-capable SOAR. With automation, there is quicker time to resolution, and the current problem of staff shortages isn’t as acute because a human spends less time with each incident.

5G Security Success

For 5G to be successful, end-to-end security from the mobile core to the edge and radio is crucial to defend against the increasing number of threats and vulnerabilities.

Designing for security in 5G networks must not only limit methods and places of attack but also dramatically cut the time between detection and mitigation. Adaptability, speed, integration, and automation are crucial features of an efficient 5G security and response system, especially considering the complexity and sophistication of 5G networks. By making security operations both predictive and automated, these features can be achieved. This approach is the most effective way to make 5G networks secure and develop trust among CSPs’ customers, which is the determining factor of the success of 5G.