www.pipelinepub.com
Volume 19, Issue 1

Security as a Differentiator for 5G

By: Eduardo Holgado

As far as consumers are concerned today, 5G is about speed and to a lesser extent latency. But is that enough to attract subscribers to new 5G networks?

Mobile operators are scrambling to roll out 5G networks at great expense. For those consumers who have done their homework, excitement about new services is high. But just like any service, 5G operators will need to differentiate their offering to compete with other 5G networks. When you ask consumers today what the greatest benefit of 5G is, they almost unanimously say that it is speed, with some adding latency to the mix and the hope that 5G will be more reliable than 4G. But with a bit more thought, many current 4G subscribers recognize that there is no need for speed beyond what they already experience.

Some educated consumers realize that the benefits of 5G will enable a new generation of applications including augmented and virtual reality tools and games, cloud gaming improvements, fixed wireless access, and others. These applications will require more speed and lower latency. But all 5G networks will promise similar specifications. So, even in the best of circumstances, 5G can easily become a commodity like its predecessors.

According to a 2022 YouGov survey, 61 percent of consumers said that they believe that 5G would improve their digital experience. But only 34 percent said they are willing to pay more for 5G. In Europe, that number drops to a mere 19 percent. This gap illustrates that consumers know about 5G and even look at it favorably. But they are still unwilling to increase their investment based on the currently perceived benefits of 5G.

5G networks are rolling out now with 5G operators promising new services that have never been seen before. These are the services that are supposed to draw consumers to the new 5G connections. But it could be years before real 5G services for consumers are available. We frequently hear about industrial and commercial 5G services that are going to be launched soon—but those don't interest consumers. So how can service providers attract subscribers to their upgraded networks, with upgraded pricing, so that they can recoup their 5G investment?

As communication service providers roll out new services that take advantage of 5G's speed and latency advantages, new challenges arise for the communication service provider (CSP) and the service subscriber.

5G challenges: secure connectivity could be the answer

First of all, consumers will consume more data. How 5G operators will cope with the elevated traffic is not within the scope of this article. But it will certainly be an issue as 5G grows in popularity, just as it was with previous generations of connectivity infrastructure. The data itself is not dangerous, but with more traffic will inevitably come more cyber threats, which will also be increasingly complex. Those threats will increase even more when 5G operators and over-the-top (OTT) vendors start to offer new services based on 5G features. As the user experience becomes more immersive, with augmented reality (AR), virtual reality (VR), and other enhancements, more new types of information, and therefore more opportunities for malicious attacks, will be pouring into the consumer's view. This could be especially true as a new service is rolling out—when there is generally some confusion about how the service works. Confusion and uncertainty are the playing fields of cyber criminals.

All indicators show that cybersecurity threats are increasing globally. The threat level will increase, likely at an even more accelerated rate, as more 5G data is consumed and more services are offered. With every new service delivered, cyber criminals will be waiting with open eyes and ears for new vulnerabilities. For example, in an environment with augmented reality, there will be new opportunities to get very influential messages to consumers as they discover new commercial and entertainment realms. As new vulnerabilities arise, the 5G operator's position as the "security hero" can be more firmly established.

Secure 5G operators to the rescue

Network operators are perfectly positioned to offer cybersecurity protection that consumers and small businesses are looking for. Every bit of Internet traffic consumed and delivered transverses the operator's network. Who better to maintain the cyber hygiene of the data than the operator? In addition, CSPs can integrate cybersecurity services into their network infrastructure and use the tools that they already have for fast, widespread provisioning of services. When a cybersecurity solution sits in the network, as opposed to the customers' end devices, it can block attacks before they reach and affect the device. Network-based cybersecurity also means that the service can be zero-touch. In other words, people are protected without having to do anything: no downloading, no installation, and no configuration necessary. A CSP's customer can simply say 'yes' to activate the service.

Moreover, subscribers actually express a desire for security to be a part of their connectivity package. With already close to one billion 5G connections, consumers are starting to experience the advantages of 5G. But they continue to be concerned about the security of their connections. They also expect their service provider to play a central role in providing that security. Results of a survey conducted by Coleman Parkes Research for Allot bear this out.

Consumer network security demands by the numbers

Fifty-seven percent of consumers said they did not know which cybersecurity solution to choose compared with 31 percent in Q4 2020. With so many potential options and features in the cybersecurity realm, consumers are confused about which solutions can actually improve their lives. This leads to a large number of consumers choosing to stay unprotected. Survey results show that 56 percent of consumers want security as part of their existing connectivity package, an increase of eight percent from 2020. In addition, 48 percent of respondents expect built-in security on their devices, compared to 27 percent in 2020. This jump of more than 20 percent shows a trend that consumers are getting more and more frustrated with existing solutions yet want to be protected without the hassle. Furthermore, 75 percent said they trust their mobile provider to protect them from cyber threats and more than 90 percent of consumers are willing to pay for cybersecurity protection.

When consumers clearly know that they want cybersecurity protection services, and they are already willing to trust their operators to provide those services, and they are willing to pay their operators for those services, it seems obvious that cybersecurity protection could be the benefit that 5G operators can offer to consumers to help them to select their network over a competitor. This is even more of an issue with 5G networks, compared to previous technologies.

For a number of reasons, 5G will be more prone to cyberattacks compared with 4G. The rise of smart devices that will be stimulated by 5G technology can translate into greater strain on Internet of Things (IoT) security. It's simple math. More IoT devices available means greater opportunities for security breaches. Additionally, a significant number of IoT devices lack built-in security, which leaves them vulnerable to malware infection. An infected IoT device can serve as a doorway to the entire network infrastructure and a widespread breach. In addition to the greatly increased number of connected devices on networks, 5G increases the threat landscape through the rise in potential points of attack with hundreds of traffic sensitive Multi-access Edge Computing (MEC) nodes, which are critical elements in delivering ultra-low latency in 5G networks. This is in addition to the greatly increased throughput per connection, which leads to more opportunities for attacks.

Though some attacks are aimed at the network and not at the consumer, the potential for consumer-focused attacks in 5G networks is also significantly increased.

A number of recent surveys show that consumers are increasingly concerned about cyberthreats. In the same survey cited above, 62 percent of consumers said that they expect secure connectivity to be a core offering from a mobile service provider. As a part of the core service offering, cybersecurity protection could be the differentiator between one 5G operator and their competitors' networks.

The difference between a secure 5G service offering and one that does not provide zero-touch cybersecurity as a part of the core offering will be a deciding factor in network selection. And now that subscribers are thinking about those shiny new 5G handsets, and the brave new world of widespread IoT, this is a good time to consider implementing a comprehensive cybersecurity solution for consumers, before they choose someone else's secure network.