WHITE PAPER

Beyond Native 5G Security: A Must for Wide Enterprise 5G Adoption

Executive Summary

Powered by the convergence of the Internet of Things (IoT), the Industrial Internet of Things (IIoT), 5G, and industry 4.0, the smart enterprise of the future is becoming a reality. Unlike previous mobile generations, which mostly targeted the consumer segment, 5G enables smart systems to share and respond to information with speed, precision, and efficiency, permitting enterprises to harness mobility to innovate, digitize, and automate their infrastructures with confidence.

5G offers a unique and valuable set of capabilities that, unlike any previous or current mobile technology, enable and expand the implementation of transformative technologies for organizations, including industrial enterprises. The value of 5G encompasses enhanced bandwidth, ultrahigh reliability, low latency, deterministic behavior, high positioning precision, and native support for machine communications that organizations across a wide range of verticals, including manufacturing, logistics, and utility companies, are looking to harness and accelerate their digital innovation efforts.

5G requires end-to-end security to ensure and maintain the secure deployment and utilization of 5G across businesses and critical use cases.

However, new technologies—especially those that enable and drive significant change—always bring new risks. As a technology that is expected to become a critical part of organizations' operational, innovation, and competitive aspects, 5G requires end-to-end security to ensure and maintain the secure deployment and utilization of 5G across businesses and critical use cases, such as augmented reality, automated guided vehicles (AGVs), safety applications, and closed-loop process control, yielding innovative and increasingly efficient operations. Whatever version of 5G infrastructure and services is used, whether public, private, or hybrid, and whatever the implemented use case, security must be in place to help protect the attack surface across augmented 5G environments.

In 5G, the Enterprise Is King

Unlike 4G, which was targeted at the consumer level, the business segment is likely to be the main growth driver for 5G consumption. Omdia Research estimates that around 70% of 5G-generated revenue will originate from the business segment.[1] In a TelecomTV survey, almost 90% of respondents believe that it will be the business segment that is likely to drive 5G ARPU growth.[2]

It is therefore important to understand how enterprises use 5G, today and in the foreseeable future, to better understand how 5G stakeholders, such as mobile operators, mobility vendors, and system integrators, can best serve their needs. Such an understanding is also essential to determine security's impact and role in facilitating 5G adoption in the business segment.

Enterprise 5G Consumption Options: Private and Slices

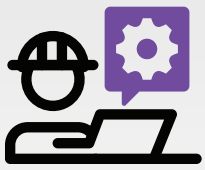
Research indicates that enterprises that consider deploying 5G will do so via nonpublic 5G networks (i.e., private 5G networks). According to ABI Research, over 90% of enterprises planning to deploy wireless technology as part of their digital transformation plan envision to deploy private 5G networks.[3] This and similar projections are supported by a stream of enterprises announcing private 5G deployments. Such an undertaking is not trivial: deploying, managing, maintaining, and evolving a private 5G network requires significant financial and human resources, and it is expected that large, well-established enterprises in leading verticals, such as manufacturing, logistics, and oil and gas, will be the major adopters in the near future. Customization, quality of service (QoS), service-level agreement (SLA) control, and system integrity (ensuring that production assets are protected in compliance with regulations) are the top factors driving these strategic and long-term investments.

The consumption of 5G network slices on top of public 5G networks is expected to gain traction once the service is commercially available. 5G network slicing is a network architecture that enables the multiplexing of virtualized and independent logical networks on the same 5G physical network infrastructure. Each network slice is an isolated end-to-end network tailored to fulfill diverse requirements requested by a particular application/use case. This will enable smaller enterprises, in addition to large ones, to take advantage of 5G by building their private customized slices to enable their use cases.

5G Is Only an Enabler for Industry Use Cases

5G is not the enterprise end game. 5G is simply a critical enabler for the real objective, which is the deployment and enablement of a great number of use cases that bring value and innovation to the enterprise. These may include such things as closed-loop process automation, real-time logistic management, augmented reality, predictive maintenance, and more. Delivery of such use cases requires the creation, deployment, and management of an interconnected 5G industrial ecosystem, including all related IoT/IIoT devices and vendors, industrial applications, and tools—both on-site and on public/partner clouds, and on the 5G network itself.

5G spectrum availability and country-specific regulations create a new balance of power in 5G's consumption by enterprises. Previously, mobile services could only be provided by established mobile operators, while in 5G, the emergence of a new ecosystem consisting of IoT/IIoT and industrial control system (ICS) vendors, mobility vendors, mobile operators, system integrators, and public cloud providers provides the enterprise with a choice as to who will deploy and manage its private 5G network.



Deploying, managing, maintaining, and evolving a private 5G network requires significant financial and human resources.

As 5G enabled enterprises to implement new critical use cases that will define its operations, innovation, and transformation, it is obvious that secure 5G-enabled use cases are required. It is the use case that needs to be secured, not only parts of its ecosystem. And meeting each use case's unique operational and security requirements and challenges should be the focus of both the enterprise and the rest of the ecosystem technologies and partners required to deliver it. This is not a one-size-fits-all challenge, and therefore security should not be designed or implemented in silos. Instead, one needs to build and deliver end-to-end security visibility, automation, and enforcement throughout a use-case attack surface as one coherent, integrated, adaptable, and self-healing security platform.

Native 5G Security Is Not Enough

5G is the most secure commercial mobile generation and wireless technology ever developed, enhancing authentication, encryption, and integrity. But an internal 5G security mechanism is only part of the story. In the TelecomTV survey, almost 90% of respondents believe that a mobile operator's 5G security value proposition is critical or very important to be successful in vertical industries.

With the increased usage and criticality of 5G in businesses, threat actors will most likely increase their focus and investment in 5G as an attack target or a way in to attack the enterprise. The 5G-enabled ecosystem that interlocks enterprises, providers, and the partners serving their unique business interests creates a distributed attack surface that 5G on its own is unable to defend. The rise of sophisticated attacks—ranging from advanced swarm attacks that will leverage 5G-enabled devices to overwhelm defenses, to increasingly sophisticated IoT/IIoT and application programming interface (API)-based attacks that can leverage artificial intelligence (AI) to speed delivery and outwit traditional and isolated security systems—warrants a defense-in-depth approach to security, one that goes well beyond native 5G security capabilities. One that builds on the foundation of native 5G security with additional security layers to protect the entire 5G ecosystem end to end to deliver business-critical enterprise use cases.

Security Foundations for Enterprises 5G Use Cases and Ecosystems

The scope of 5G usage in the business market will evolve as 5G technology, services, and deployments evolve. Security must be an enabler for such evolution and accompany it, not follow, so it does not become an afterthought, considering the potential criticality of 5G for businesses.

A security infrastructure capable of enabling enterprises a secure 5G consumption and enablement should integrate the following characteristics:

Broadness: With a rich scope of possible 5G-enabled use cases in different enterprise verticals, it is the security of the use case itself that is the objective. As a use case requires more than just 5G (5G-enabled IoT/IIoT/applications are other example of components required for a use case), the security infrastructure in place must be broad enough to holistically cover the end-to-end use cases' ecosystem.

Visibility: You cannot protect, you cannot react to threats, and you cannot properly evolve if you do not know what is going on in your network, your applications, your services, and your ecosystem.

Knowledge: The quantities of data and events are already overwhelming the enterprise and providers, and 5G will only make it worse. AI-based and automation tools must be put in place to gather, analyze, correlate, and make sense of all that data to be able to take rapid action in the face of threats and attacks. The decision to act must be based on the largest possible set of data as context and reliable, up-to-date threat intelligence will be crucial in reducing false positives.

Security must be an enabler for such evolution and accompany it, not follow, so it does not become an afterthought, considering the potential criticality of 5G for businesses.

Controls: Control, or enforcement, is the ability to take an action where and when required to minimize the impact of a threat, throughout the 5G ecosystem attack surface. Such an action can be the result of local visibility, threat intelligence, and automation, or it can be acted upon by security management and operations and higher-level orchestration tools.

Security needs to span both the enterprise and the 5G provider, both public and nonpublic 5G networks. It ought to span the enterprise operational technology (OT) and information technology (IT) environments. It should span the 5G radio network, the edge compute sites, and the 5G core. It needs to be able to take automated decisions and actions based on analytic and AI tools. It must be built as an architecture that allows native integration and flexibility to adapt to specific industrial use cases and requirements and the very high performance and low latency required by 5G.

[1] Aditya Kaul and Mark Beccue, "Artificial Intelligence for Telecommunications Applications Report," Omdia, 3Q 2019.

[2] "TelecomTV 5G and Security Survey: Leveraging Security to Capture the 5G Business Market," TelecomTV, February 26, 2020.

[3] "Nokia & ABI Research: Enterprise Digital Transformation Through Industry 4.0," GSMA, May 6, 2020.

FORTINET

www.fortinet.com

May 21, 2021 9:24 AM

1007364-0-0-EN