POINT OF VIEW

Why Cybersecurity Is a Condition for 5G Success

Executive Summary

5G technology holds high expectations to enable new possibilities and experiences for consumers, enterprises, and societies. More than ever before, mobile technology has the potential to profoundly impact the possible. This has not yet happened for several reasons (technological, operational, and commercial). 5G will be most impactful for enterprises of all sizes and sectors as it will empower innovation throughout product and service life cycles.

However, new technologies—especially those that enable and drive significant change—always bring new risks. As 5G technology, networks, and services become a precious and critical resource they will become honeypots for threat actors. With 5G's growing reliance on standard IT technology, open and distributed architectures, and multivendor value-add service ecosystem comes a growing attack surface and greater facility for threat actors.

The above has not been ignored: 5G standards, 5G providers, enterprises, and regulators have, and are, taking their part in trying to reduce 5G-related risks while establishing best practices and procedures to deal with eventual attacks and their consequences.

5G cybersecurity solutions provide the required visibility, enforcement, and automation to complement and enhance native 5G security mechanisms, respond to enterprises' security demands, and help operators and enterprises remain compliant today and in the future.

85% of operators rank security investments as the #1 operational priority to help achieve their long-term enterprise revenue goals.[1]

Building Enterprise Trust Is Key to 5G Service Consumption

According to the GSMA Intelligence Operator in Focus: Enterprise Opportunities 2021 survey, security saw the strongest growth in demand from enterprises; it was highlighted as the primary growth area by 44% of operators surveyed.[2] The survey also saw investment in security as the #1 operational priority for operators to help achieve their long-term enterprise revenue goals. Keeping the customer within the operator's domain as long as possible while consuming as many services as possible is the goal.

To achieve this goal, trust must be established and can only be as strong as the operator's ability to provide and demonstrate resilience, integrity, and privacy throughout its value, from connectivity to use cases, applications, and platforms. Cybersecurity capabilities play a role in an operator's ability to do so and should be complemented by a set of consumable security services to allow enterprises to achieve their security posture, practices, and compliance.

Security Considerations Beyond Native 5G Security

5G is the most secure mobile technology ever, but its security is not complete nor is it bulletproof. Significant progress was made in providing better authentication and privacy via the growing use of encryption and authentication between critical components and network functions (NFs) in the 5G system (5GS). Although this helps to protect against certain types of risks and provide better privacy, they do not address other important threats and attack vectors, such as:

- 5G Core and RAN functions are becoming cloud-native, enabling open interfaces, flexible architectures, microservices, and cloud-based deployments. This evolution impacts the security posture of 5G networks as cloud security best practices, multi-layer security controls, zero-trust architecture (ZTA), and cloud ecosystem security must be considered.
- The ongoing cloudification and standardization in the access (RAN) and core components create a 5GS that is multivendor (existing and new), open, and distributed, where ZTA, supply chain, and API cybersecurity considerations are needed.
- Driving growth is achieved by providing more value to consumers and enterprise verticals—value that goes beyond mobile connectivity. This includes applications and partner ecosystems for different verticals and use cases, which emphasizes cybersecurity from the user plane function (UPF) to the application and service regardless of their location.
- 5G multi-access edge computing (MEC) capabilities play a crucial role in delivering new use cases, reducing transport costs, enhancing scalability, and more. Edge sites are multitenant, hybrid-cloud environments, containing various control and user plane components. Such a high-value multitenant environment must encompass cybersecurity best practices, including segmentation, API and application security, perimeter security, and zero-trust architectures.
- With the hunt for enterprise high-value business, organizations need to consider their ability to comply with general and industry-specific regulations. Their consumption of high-value, critical 5G services and use cases will depend on their ability to meet compliance. The 5G providers' cybersecurity capabilities have an important role in providing the customer cybersecurity visibility, control, compliance analysis, reporting, and possibly, mitigation. These are crucial advantages and enablers in enterprises' 5G adoption.

The Unique Case of Private 5G

Private 5G technology is not very different than public 5G technology. The differences between the two are mostly around scalability and some architectural aspects. Industrial verticals and enterprises are already implementing private 5G networks. These environments are characterized by assets (sensors, actuators, valves, etc.) that work together with industrial control systems (ICS) to control physical processes. All these components working together are known as operational technology (OT). Security in OT environments is governed by specific industry regulations, many of which are driven by the Purdue model (IEC 62443-ISA99), created before private cellular was available to enterprises.

The introduction of private 5G networks into industrial/OT environments can violate the Purdue model and render it incomplete. This seems to be unique to private 5G use cases and requires appropriate OT cybersecurity visibility, control, and reporting as part of a private 5G network in OT environments and use cases.

Cybersecurity Simplification: from Silos to Converged to Integrated Platforms

The 5GS is complex, open, distributed, and agile. The complexity is overcome by the management, administration, and orchestration tools used to automate and orchestrate the different 5GS components to deliver a required service, SLA, and use case. Adding cybersecurity must rely on architectures that move away from siloed, point products to a set of converged products that work together to create a cybersecurity platform. Interworking and orchestration within the platform should be available natively and via the use of cybersecurity artificial intelligence (AI) and orchestration tools. Such an architecture and capabilities will ensure that agile and adaptive cybersecurity, in all its guises, is available for internal and external use.

Operational technology (OT) cybersecurity must be incorporated in private 5G networks in industrial environments.

Fortinet Cybersecurity Mesh Platform for Public and Private 5G Networks and Ecosystem

The Fortinet Security Fabric is the leading cybersecurity mesh platform where converged and integrated cybersecurity products deliver modular user and control plane security in 5G networks and ecosystems.

5G network user plane security: From the RAN and onto the application, the user plane is the most risk-exposed, high-value component in the 5GS and ecosystem. The Fortinet Security Fabric provides security gateway (SecGW/SEG), next-generation firewall (NGFW), carrier-grade NAT(CG-NAT), and application-level cybersecurity automation and reporting.

5G network control plane security: The control plane extends beyond the 5G Core into the RAN and its diverse architectures, the O-RAN real-time intelligent controller (RIC) environment, the northbound interfaces to OAM tools, and exposed interfaces, such as the network exposure function (NEF). The Fortinet Security Fabric provides security segmentation, API security, and SecGW/SEG functionalities along the control plane.

Mobile edge security: 5G MEC is a complex environment. It is an application-rich, dynamic, resource-limited, multivendor, multitenant cloud environment. MEC may also include user and control plane elements, such as RAN CUs/DUs, O-RAN RICs, and UPFs. The Fortinet Security Fabric meets the complexity, importance, and resource limitation of the MEC via leading energy- and space-efficient solutions that deliver platform cybersecurity, segmentation, and control and user plane cybersecurity.

Private 5G cybersecurity in industrial environments: The Fortinet Security Fabric provides native OT cybersecurity that can be implemented as part of the 5G user plane and edge cloud security.

Conclusion

With great expectations comes great responsibility. 5G's great expectations are gradually turning into reality as 5G systems and ecosystems implementations are fulfilled and evolving. These capabilities enable new use cases and empower entire industries. A great responsibility resides with 5G providers to deliver on trust and compliance as a cornerstone for 5G consumption and fulfillment, enabled by converged and integrated cybersecurity platforms embedded into the 5G fabric and ecosystem.

[1] Sylwia Kechiche, Andrey Popo, "Understanding operator thinking, expectations and agendas," GSMA Intelligence, Sept. 2021.

[2] Ibid.

FORTINET

www.fortinet.com

February 10, 2023 1:58 PM
1963469-0-0-EN