WHITE PAPER

Cybersecurity Could be Mobile Providers' Secret Ingredient to Drive Enterprise 5G Adoption

Introduction

Beyond consumer-facing 5G services, 5G promise and monetization has fallen short of the world changing, billions-dollar hopes around industries' digital transformation.

The path forward is going beyond B2C and into B2B and B2B2X models and services where 5G facilitates new use cases that are focused on industry verticals' specific environments and needs. There is a growing understanding that the bigger value a mobile provider can provide lies in helping the enterprise solve business problems via the evolution of 5G from a network into a platform encompassing connectivity, services, applications, and use cases.

Cybersecurity is an important accelerator and differentiator for mobile providers to gain their enterprise customers' trust and business as 5G use cases will serve as the foundations for their evolution and commercial success.

A 5G platform should incorporate cybersecurity visibility, enforcement, reporting, and automation as an addition to native 5G security to meet enterprise verticals and regulators security and compliancy requirements.

Adding cybersecurity to any 5G platform is critical:

- Enterprises 5G-enabled use cases are critical to their operations and success.
- Native 5G security is focused on 5G network functions internetworking.
- 5G is one component within a larger ecosystem that must be secured.
- 5G can be hybrid, distributed, and exposed throughout the 5G ecosystem

Cybersecurity investment in any 5G platform is an enabler:

- Security is a top challenge for enterprises in adopting innovative technologies (Verizon 5G Business Report, December 2020).
- Security and compliance are top challenges/barriers to enterprise 5G adoption (Verizon 5G Business Report, December 2020).
- Mobile providers consider security investment as very important in achieving long-term enterprise revenue goals (GSMA Intelligence Operators in Focus: Enterprise Opportunities 2021).

A cybersecurity platform for the long term

The implementation and delivery of any 5G platform, its capabilities, technologies, solutions, and services will continue for years to come and therefore dictates a phased evolution of the cybersecurity foundation and services that must accompany it. Mobile providers must think strategically and for the mid to long term when it comes to their cybersecurity investments. They need to invest s a cybersecurity platform that will provide them multiple degrees of freedom, to adopt to their evolving ecosystem, customers, and the use cases they provide:

- Scaling and performance freedom: Number of connected sites and devices, high bandwidth, ultralow latency.
- Form and customer freedom: Physical, virtual, containerized, multitenant
- Location freedom: Customer premises, MEC, public cloud, data center
- Hierarchical freedom: Device, network, application, service-level security
- Service freedom: As part of a service/use case, as a revenue-generating value-added service (VAS)
- Operational freedom: Management, artificial intelligence (AI)/machine learning (ML), security operations center (SOC), automation

When a security platform such as the Fortinet Security Fabric offers these degrees of freedom and flexibility, it avoids the trap of silos and isolated security solutions. It enables a common, end-to-end security that empowers gradual and modular deployments of security with ease of integration, rapid deployment, simplified operations, and enhanced return on investment

Evolution, not revolution

Enterprise-facing 5G services and use cases will materialize and evolve with time, and with it, so must the cybersecurity platform and its services. Once a modular and evolutive security platform has been identified, such as the Fortinet Security Fabric, one needs to consider the security implementation evolution and priorities: Where do we start to secure the existing 5G ecosystem and use cases, and how do we evolve with private and public 5G deployments, MEC deployments, advance

5G service availability, and use-case evolution?

Figure 1 identifies three key security priorities that specifically deal with the expected evolution of 5G-enabled enterprises

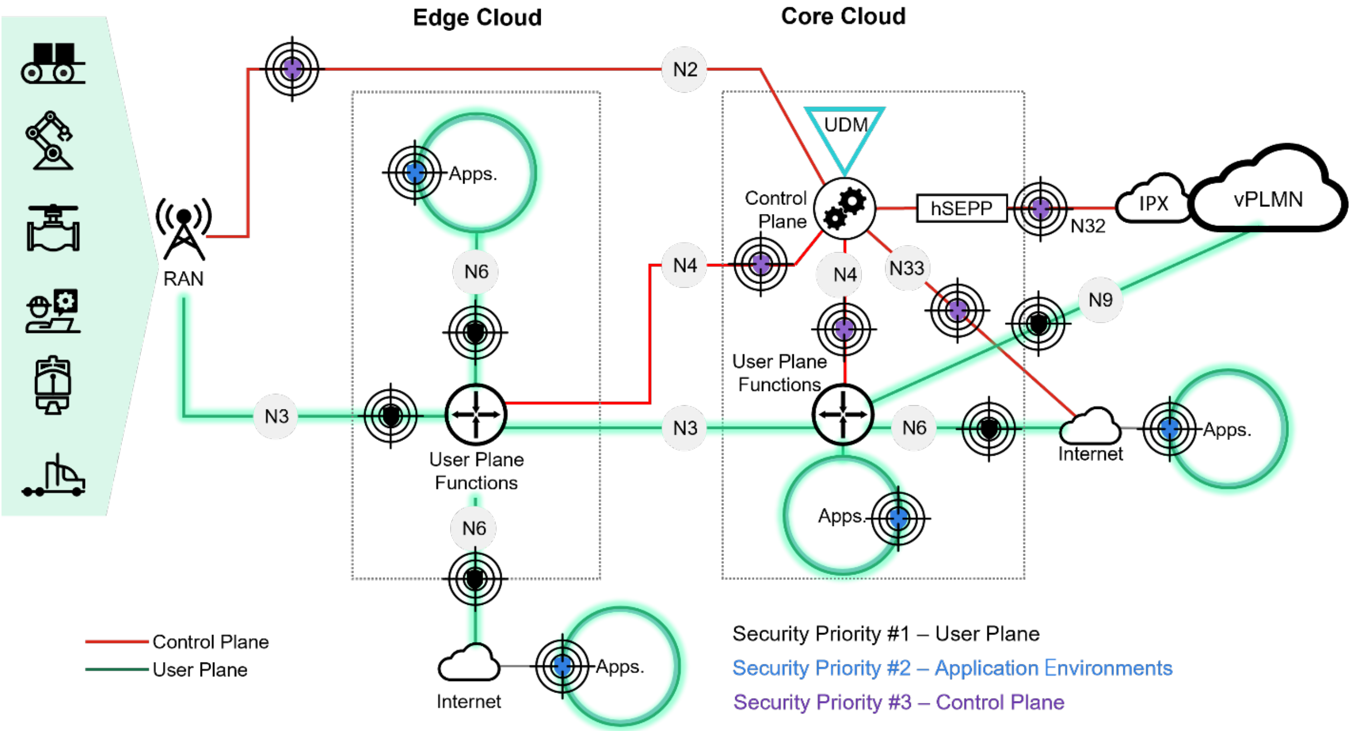

Figure 1: 5G security priorities.

Priority #1 – user plane/user data security

The consumption of 5G (private, public, and hybrid) in the enterprise enables a set of operational innovations and benefits. These rely on the reliable and continued exchange of data between endpoints (IoT, IIoT, OT devices) and applications, regardless of their location (enterprise on-premises, national and international distributed, MEC, DC/private cloud, public cloud).

Therefore, the first and immediate priority should be the security of the user plane data in any type of 5G deployment and use case, as shown in Figure 1.

Securing the user plane data should encompass the following:

- Secure the data traffic from the radio access network
- Secure the data as it is distributed to applications and their environments in the MEC and elsewhere
- Segment the data flows to avoid threat lateral movements and limit potential attack damage

Both enterprises and 5G service and solutions providers see the need for an enhanced 5G security as an integral part of any 5G delivery and consumption ecosystem.

- Secure external data network connectivity and exposure, including roaming partners for internationally connected devices and distributed enterprise environments
- Ensure that data and behavior anomalies are identified and will not affect the 5G service delivered

Priority #2 – application and compute environments security

Digitization, connectivity, and automation are at the core of the transformation journey enterprises are embarking on and applications, cloud technologies, AI/ML, DevOps methodologies, and other components are the engines driving them.

Securing the applications and their compute environments, independent of their location or provider, is critical. This should encompass the following:

- Application-level security
- Application programming interface (API) interworking security
- Zero-trust access control
- Security segmentation
- Continuous integration/continuous deployment (CI/CD) pipeline security integration

When a security platform such as the Fortinet Security Fabric offers these degrees of freedom and flexibility, it avoids the trap of silos and isolated security solutions.

Priority #3 – control plane security

The control plane is at the heart of 5G's capabilities and services, public and private. Its key role made it the focal point for 5G native security and has made this environment a secure one. However, the control plane is connected to external environments that can, accidentally or not, serve as attack vectors.

The distributed and open nature of 5G and its deployment in enterprise environments and use cases will increase the control plane potential exposure via network exposure function interworking and the sometimes physically unsecure nature of the 5G radio network.

The growing number of connected users and devices, the ever-increasing traffic volumes and their critical importance, and the distributed and open nature of 5G and the large attack surface it creates will trigger significant growth in security events.

As the control plane environment is considered the most secure part of the 5G network and some of the external interworking it offers is not commercially available today, we consider securing this environment as important and urgent for the exposure point already in production use, such as the control plane—radio network interworking and control plane—user plane interworking.

Securing the control plane should secure these exposure points:

- Control plane to radio access network (RAN) security
- Control plane network exposure function API security
- Control plane to user plane security
- Control plane to roaming partner security

Security Operations

The growing number of connected users and devices, the ever-increasing traffic volumes and their critical importance, and the distributed and open nature of 5G and the large attack surface it creates will trigger significant growth in security events. These must be dealt with quickly and efficiently to maintain the 5G network and services available, scalable, and agile.

Empowering the MNO SOC to deal with the expected growth efficiently and effectively, the following principles must be put in place:

- End-to-end visibility (network, compute, applications, users)
- Zero-day attack protection and decoys to proactively discover lateral movements
- Unified events correlation
- AI and ML data analysis for events investigation and mitigation
- Closed loop automation

The growing number of connected users and devices, the ever-increasing traffic volumes and their critical importance, and the distributed and open nature of 5G and the large attack surface it creates will trigger significant growth in security events.

A Security Platform as an Enabler for Enterprise 5G Adoption

The security of any 5G platform is only as strong as its weakest link. The above and other security considerations should be structurally, methodologically, and proactively implemented as an enabler for enterprise adoption. MNOs need to consider a holistic, end-to-end security implementation that is preferable due to the distributed nature of 5G networks and services, the strong interworking between them, and the unique industrial ecosystem required by enterprise use cases.

A strong SOC with a rich set of visibility, correlation, analytics, and automation capabilities is mandated to handle significant amounts of incoming security data and turn it into actionable insights and enforcement. The Fortinet Security Fabric provides a standard set of security visibility, control, and management throughout the public and private enterprise 5G ecosystem—from the RAN, through the core and edge compute environments and applications, and to the private/ public cloud and third parties—to provide mobile operators a security platform that enables modular and gradual security for private and public enterprise 5G consumption.

April 12, 2023 12:11 PM

wp-Cybersecurity-Could-be-Mobile-Providers-Secret-Ingredient-to-Drive-Enterprise-5G-Adoption

2080801-0-0-EN