WHITE PAPER

Security for the Telco Cloud: Challenges and Solutions

Introduction

A mobile network operator (MNO) business is, by default, bounded by its technological foundations and capabilities. For over three decades, MNO business was built upon and defined by the following technology attributes:

- **MNO-specific and legacy technology and protocols**
- **Hardware-based, monolithic infrastructure**
- **Siloed and separated technological islands**
- **Legacy operational and back-end applications**
- **Specific service-level agreements (SLAs) and compliancy**

As business, competitive, and technology environments are often undergoing rapid digital transformation, the reliance on such legacy technologies and architectures can no longer sustain an MNO's ability to stay relevant and drive innovation and growth. A foundational evolution is required—the evolution to the Telco Cloud model.

The Telco Cloud is an industry term used to describe the new foundation upon which an MNO's ability to profoundly change how they operate is enabled. The Telco Cloud is not a single product or technology, however, but a vision and an objective that is enabled by a set of cloud technologies. A Telco Cloud empowers an MNO's ability to drive efficiency, agility, value to the customer, service innovation, and overall growth.

As suggested by the name, the Telco Cloud is focused on the implementation, standardization, and use of cloud technologies specifically in Telco environments.

This reliance on cloud technology, at its core, provides significant advantages:

- High levels of automation
- Agility and flexibility
- On-demand scalability
- Rapid innovation and go-to-market
- Flexible consumption models

The advent of 5G is driving organizations toward edge compute and edge services, resulting in an expanded attack surface while threats continue to increase in sophistication. This coupled with the desire and ability to provide value beyond mere connectivity to the business market—it is also clear that security must play an important role in the Telco Cloud.

There are two aspects of Telco Cloud security that need to be considered:

Security for the Telco Cloud: Ensuring that the technologies, applications, and services that make up the Telco Cloud service platform are properly secured to ensure availability and service continuity.

Security from the Telco Cloud: The Telco Cloud as a service platform, enabling the provisioning and delivery of security services to internal and external customers.

Telco Cloud Components, Architecture, and Security

For the Telco Cloud to be the platform for innovation and growth for MNOs, it must be able to provide the highest levels of flexibility, agility, and openness—and therefore, it must rely on the following technology pillars:

- **Software-defined networking (SDN)** technologies provide an abstraction of network resources—providing high flexibility, reducing hurdles to innovation, and ensuring the elasticity of resources.
- **Virtual and containerized network function (VNF and CNF)** technologies decouple network services and functions from hardware platforms. This provides cost reductions and flexibility while enabling enhanced agility and the ability to introduce new functionalities and value.

- **Openness via application programming interfaces (APIs)** enables the rapid and cost-effective integration of third-party applications and associated services to drive innovation and competitiveness.
- **DevOps** technologies empower the MNO to deliver and update its own applications, services, and innovation, rapidly and dynamically enabling a better response to market demands and competitive pressures.
- **Consumption as a service ("aaS")** transforms capital expenditure (CapEx) investments into smaller, recurring operating expense (OpEx)-based revenue streams.

The Fortinet Security Fabric Foundation for Telco Cloud Security

The Telco Cloud journey is all about the implementation of the above technologies in an integrated manner to offer a single, seamless service platform. For this to work as effectively and efficiently as possible, security should be integrated into and be part of the Telco Cloud, creating a seamless, integrated security platform. This is the foundation of the Fortinet Security Fabric Platform.

The Fortinet Security Fabric cybersecurity platform is built around a broad set of security technologies that have been fully integrated and automated—enabling communications service providers (CSPs) and enterprises to accelerate digital innovation efforts while simultaneously reducing complexity and risks.

The Fortinet Security Fabric follows the same technology principles that are the foundation of the Telco Cloud—SDN, VNF/CNF, openness via APIs, and security operations (SecOps)—implemented with support for MNO-specific requirements, such as massive scalability, efficiency, high performance, and very low latency. Like the Telco Cloud, Security Fabric components are internally integrated to form a seamless and automated security service platform, and externally integrated into the Telco Cloud technologies, components, and architectures to become a seamless part of the Telco Cloud itself.

Its internal and external integration via APIs into a large technology partner's ecosystem enables an agile and transparent security evolution alongside the Telco Cloud evolution in terms of technology, service platforms, and applications to address the dynamic risk environment.

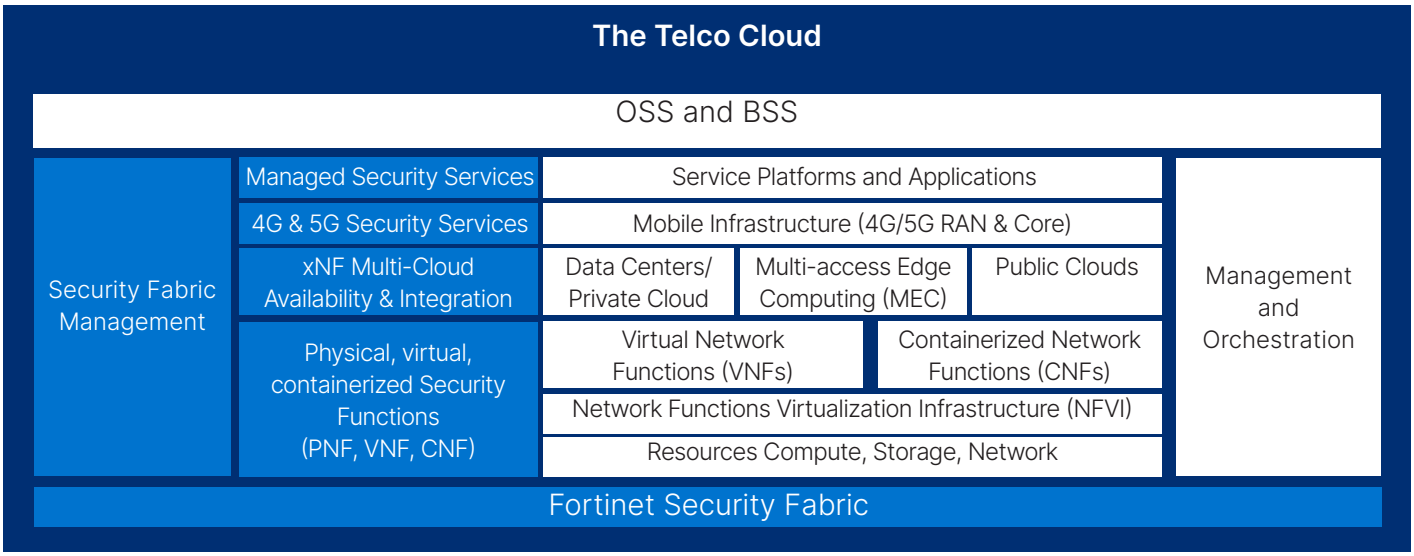

Figure 1: Telco Cloud and Fortinet Security Fabric Platform

Security Platform for the Telco Cloud

Network functions and their different form factors (physical network function [PNF], VNF, and CNF or xNF) are the basic building blocks of both the Telco Cloud and the Fortinet Security Fabric. Based on the seamless combination of underlying technologies with location and service requirements, the Fortinet Security Fabric enables the MNO to deploy the appropriate xNFs that are best suited to provide their required security visibility, control, and protection.

The Fortinet Security Fabric covers the following aspects:

1. **Multiple layers** provide security visibility and control at the management and orchestration (MANO), physical, and virtual infrastructure, user-plane VNF/CNF, control-plane VNF/CNF, and network operations center (NOC) and security operations center (SOC) layers.

2. **Multiple domains** are applicable in multi-access edge computing (MEC) data centers and private and public clouds.

3. **Multiple network functions and tenants** are applicable for different network slices and use cases.

4. **Continuity across time** with integration with orchestration and DevOps processes, and into its continuous integration/continuous deployment (CI/CD) pipeline, the Fabric provides continuous protection throughout the network evolution life cycle.

Security for the User and Control Planes in a Mobile Infrastructure

The Fortinet Security Fabric also provides security for 4G and 5G infrastructures for both the user and control planes via the deployment of two types of xNFs: The FortiGate next-generation firewall (NGFW) and the FortiWeb web application firewall, which are cross-integrated to provide a wider security context and visibility, achieving automated and enhanced security for the infrastructure's exposure points:

- Long-Term Evolution (LTE) and NR to EPC and 5GC via security gateway (SecGW) functionalities, and deep packet inspection for GTP-U, GTP-G, and Stream Control Transmission Protocol (SCTP) with high performance and ultralow latency.
- Packet data network (PDN) connectivity from the EPC, 5GC, and MEC with Carrier-Grade Network Address Translation (CGNAT) and full NGFW security services.
- Roaming interfaces between home and visited PLMNs.
- API exposure points in the 5GC (through the NEF) and MEC security, with API schema and value validation and enforcement, API GW functionalities, HTTP/2.0, and application-level attacks.

Security for Service Platforms and Applications

Service platforms and applications are the engine for revenue-generating services. Although such services delivered are mostly consumed via 4G/5G infrastructures, they cannot rely on security for the mobile infrastructure due to their unique environment and risks, including:

- Exposure to application-level attacks
- A DevOps environment with a CI/CD pipeline as the backbone for service innovation and delivery

The Fortinet Security Fabric enables MNOs to deploy FortiWeb and FortiGate xNFs to ensure:

- Artificial intelligence (AI)-powered protection against Hypertext Transfer Protocol (HTTP) and application-level attacks (OWASP Top 10)
- API protection with microservice-based applications
- Container-based security policies for north-south traffic
- Integration with Service Mesh Interface services (such as Istio) for east-west container traffic visibility and security enforcement
- Security integration in CI/CD pipelines, container registry image scanning, ingress/egress security, and east-west containers traffic visibility and control

Security for a Multi-cloud Environment

One of the central benefits of the Telco Cloud is its ability to take advantage of multi-cloud environments and services to maximize efficiency, scalability, agility, and cost.

A mix of public clouds, alongside the MNO's private clouds, can be used to deliver service platforms and applications, parts of the 4G and 5G infrastructure, MEC network functions virtualization infrastructure (NFVI) environments, and more. It is therefore important that the Security Fabric extends its security capabilities to these environments:

- Security xNFs are integrated and available for all major public cloud providers
  - Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud Infrastructure (OCI), Alibaba Cloud
- Microservices and Kubernetes public cloud support
  - AWS EKS, GCP GKE, Azure AKS, OCI OKE, Native Kubernetes
- Public cloud infrastructure visibility and control

Security for MEC Environments

MEC sites are crucial in bringing services, functionalities, and applications close to the end-user, whether it is a business, a consumer, or an Internet-of-Things (IoT) device. This is a building block in the MNO's ability to deliver 5G's uRLLC-type services and provide a cloud environment for the deployment and delivery of edge applications.

MECs can be implemented via the MNO's own internal cloud technology/environment, such as OpenStack, VMware, and Kubernetes, or it can deploy public cloud solutions for MEC—such as AWS Wavelength and Azure Edge Zone.

The MEC, therefore, can be a mix of multiple technologies and components:

1. 5G user-plane function with PDN breakout
2. NFVI environment and components (compute, storage, networking)
3. Service platforms and applications components
4. Host environment to partners and third-party applications

The common Security Fabric xNFs, FortiGate and FortiWeb, are sufficient to safeguard what may be a complex MEC environment:

- Protect the user-plane termination from the radio access network (RAN) and PDN connectivity
- Integrate with a large set of NFVI environments, both private and public
- Secure any API exposure point in the MEC
- Protect the service platform and application components
- Provide security visibility and control for a MEC microservices environment
- These services must be provided via a small xNF form factor due to the limited amount of local resources.

Security Management for the Telco Cloud

The Fortinet Security Fabric's Telco Cloud security platform provides protection of the MANO layer against both external and internal attacks. It also allows multiple integration routes to the Telco Cloud MANO system:

Direct connectors via RESTful APIs between MANO and the Security Fabric so that security xNFs are aware of all virtual machines (VMs), pods, VNFs, and CNFs that are deployed

Integration of the Security Fabric as a VNF Manager (VNFM) to MANO, so that security xNFs can be deployed, scaled, and upgraded as VNFs or CNFs for tenants in an automated manner

The Fortinet Security Fabric provides the following capabilities:

- Security Fabric centralized management via a single-pane-of-glass management system for comprehensive visibility
- Continuous risk assessment and compliance reporting (National Insitute of Standards and Technology [NIST] and Center for Internet Security [CIS]) covering misconfigurations and improper connectivity
- Scanning of container and VM images for vulnerabilities before they are deployed
- Integration into the DevOps environment and the CI/CD pipeline to ensure continuous security protection even when network functions are upgraded, and services evolve over time
- Perimeter firewall for the MANO and NFVI layers
- Real-time monitoring and reporting
- Real-time indicator of compromise (IOC) detection
- Task automation
- Security information and event management (SIEM)
- Analysis of different events and logs with AI and machine learning (ML)

Conclusion

The successful transition to a Telco Cloud operational model demands profound change, new expertise and mindset, and considerable investments. This transition, however, is strategic to the evolution and success of the MNO, and as such, seamless security should be integrated as part of the Telco Cloud overall ecosystem to help safeguard availability, integrity, and business continuity.

The Fortinet Security Fabric provides a seamless, integrated, and automated security foundation for the Telco Cloud—providing a framework to secure its technology and its service and operations domains with unparalleled flexibility. It does this by providing multilayer, multidomain, multitenant, and time-continuous security visibility, control, and protection.

Further, the Fortinet Security Fabric not only secures the Telco Cloud but it also provides a multitenant, security monetization platform, allowing MNOs to deliver value-add, competitive, and revenue-generating security services to their business customers and their unique use cases.

June 2, 2021 6:49 PM

C:\Users\cyan\Documents\Creative Services - Misc\Document Edits\wp-security-for-the-telco-cloud-challenges-and-solutions\wp-security-for-the-telco-cloud-challenges-and-solutions-060221

861999-A-0-EN