SecurityGen
Telecom Security. Transcending Generations.

TELCO WORKLOADS IN HYPERSCALER CLOUDS SECURITY IN THE 5G CONTROL ROOM

One of the dominant trends of the last decade in the telco industry was network function virtualization and cloudification, closely connected with 5G that came to the spotlight just a bunch of years later. But in the last ten years, the broader ICT industry has also witnessed the unstoppable growth of public cloud providers. The first wave of telco workloads (e.g., functions of EPC, 5GC, IMS, and O-RAN) was designed for the Telco Cloud, built on purpose infrastructure run by telecom operators. Today, it seems natural that telco workloads can and will run more and more in public clouds too.

Is security entirely under control in this landscape? Do best practices of the IT and cloud industries offer full coverage for troubles a telco workload can meet?

1. Telcos and Hyperscalers: still different but closer and closer

At the beginning of the Cloud era, Telcos explored the possibility to reap fruits from this new business opportunity selling directly to customers their own cloud services. More than a decade of experience taught us that this industry is nowadays characterized by a sharp border between the role of the Telcos and the role of the Hyperscalers, companies who made it grow until a nearly unreachable level of economy of scale in the deployment of worldwide spread data centers. Of course, I am talking about the usual suspects, Amazon Web Services, Google Cloud Platform, and Microsoft Azure, even if we must not forget about a player like Alibaba, with a dominant role in the Chinese market. Telcos tried hard to turn their expertise in homegrown data centers into a business, and there is still a bunch of Telco Public Clouds out there, but it is today clear that taking the role of an Hyperscalers is impossible for a Telco.

Someone might object that borders between Telcos and Hyperscalers are not sharp anymore, but actually blurred today and doomed to be more and more so in the future. Sure! Already with CDNs, Telcos understood that their proximity to users is an asset, but this use case is not enough to justify the strong tide pushing Telcos and Hyperscalers to cooperate. Only with Multi-access/Mobile Edge Computing and the promised land of 5G use cases in mind one can figure out why the industry is in such turmoil.

2. Telcos' enterprise IT side: the paved road to Hyperscaler clouds

A telecommunication company, seen as a private technology-driven enterprise, has many IT needs addressable with tools available at Hyperscalers.
The first and the most obvious is the wide variety of computing and storage models (technical and commercial), sweeping away the following Telcos' headaches related to hw:

- Fast obsolescence cycles (much work for procurement);
- Need for flexibility against highly unstable workloads (planning is complex);
- Bottom position in the value chain (applications are the real moneymakers).

And while Telcos initially approached Hyperscalers for very limited infrastructure-procurement-related issues (e.g., finding resources for test environments), the general consensus is now achieved on the many business and technology use cases a Telco could transfer partially or totally to a Public Cloud. A partial list includes:

- Digital channels, commerce, and customer experience platforms;
- Business processes and Digital BSS;
- A lot around billing;
- Operation processes and Digital OSS;
- Analytics (all sort, for CRM, for predictive maintenance, anti-fraud, etc.);
- Machine-learning tasks (especially the training bit).

3. Telcos' specials

What is left then at the very heart of a Telco? What peculiarities make the Telco industry unique for an Hyperscaler, compared to a generic large enterprise customer? We need to consider at least two crucial aspects.

First of all, access and proximity to customers. The access networks coupled with many points of presence, from towers to metro and regional Central Offices, are a crucial asset for the successful implementation of the most demanding 5G use cases, based on ultra-low latency, often coupled with large bandwidth. All Hyperscalers claim to be getting closer and closer to the network edge, where the Telcos' IP pipe terminates, either spreading their own DCs' geographical footprint and/or directly partnering with Telcos to build MEC DCs at Telco's locations (examples are AWS Outpost and Wavelength, Azure Edge Zones, Google Distributed Cloud). Simplifying the picture, in this marriage, the Telco brings the IP pipe and the sites, the Hyperscaler its ability to build a Data Center infrastructure, its ecosystem of apps, and the capacity for orchestrating and moving workloads around.

The second aspect, access and core networks, respectively the entry and the control point of the IP pipe, are primarily in the hands of Telcos: do not be surprised to find access networks there, just think about the Open RAN wave. Access and core networks are made of telco workloads, and here we get to the point: with a foot at the network edge, an Hyperscaler can propose a telecom operator to take the infrastructural burden of all telecom workloads, also of the most demanding user-plane ones.

4. Building telco workloads

Which options do Hyperscalers have to approach the network function side of the story?

1. Propose their own stack

The hyperscaler can propose its own product, self-developed or put together with some partners, to the market. This approach seems to be appealing for private 5G networks (see AWS Private 5G). In this case, the Hyperscaler becomes a direct competitor of telecom operators. National spectrum licensing regulations are, of course, a pre-requisite for this model.

2. Acquire a vendor and add it to their portfolio

The Affirmed and Metaswitch cases. For example, a light MVNO could directly think about buying core network functions as cloud services without building a physical on-prem core network.

3. Invite major technology vendors to certify deployments on their stack

This approach makes much practical sense. Most of the prominent technology vendors are simply too experienced and have too much influence and footprint in the industry to think you can avoid them. But these same players understand that their final customers, the Telcos, won't let them play alone in Telco Cloud silos forever. In this case, the technology vendor will leverage at least IaaS and CaaS services (VM and container services) provided by the Hyperscaler and let the telecom operator be free to choose a Hyperscaler as a partner.

4. Invite technology vendors to develop network functions with Hyperscalers' tools

Beyond IaaS and CaaS, load balancers and a large variety of DB types are already what is needed for a 3-layer decomposition (load-balancing, signaling front-end, context, and stable data back-end DB) of network functions. A more profound decomposition into microservices can be supported by service mesh frameworks (GCP Anthos Service Mesh, AWS App Mesh), message queuing, and API management services. A countless number of other solutions are available for other ancillary but critical functions, like observability, configuration automation, CI/CD processes, etc.

Though really fascinating, it is too early to bet on the success of such an approach: massive vendors prefer to have complete control on the internal sw architectures of their network functions, for performance and assurance reasons at least.

5. Security of Telco workloads

Whatever the approach to telco workloads is, security becomes a shared responsibility in case of deployment at an Hyperscaler cloud. The Hyperscaler will do its best to ensure that the cloud itself is safe, together with all the tools in its portfolio; the telco workload's and the network function's security is instead the final concern of both the technology provider and of the telecom operator. The literature about best practices for cloud security is enormous. Nevertheless, a few principles stand out:

- Trust no one/nothing;
- Use as much automation as you can;
- Audit/analyze/inspect what you do.

The "trust no one/nothing" is enforced, for example, with a strong identity and access management, encryption of communications (TLS) and data (at rest and in transit), and also with traditional network and application-level tools (network segmentation, IP firewalls, WAF, etc.). Sometimes, these techniques can be pushed inside the service mesh implementation, e.g., see some of the Istio features.

Automation must back all inspection tools used to verify the correct implementation of security measures at all levels, from VM images to complex as-code templates.

Regular audits, log analyses, and inspections help highlight threat exposures and gaps in the security posture. On one side, you need to see your environment with the eyes of a hacker, performing audits aiming at breaching through defenses. On the other, you need full traceability of events and advanced analytic tools to spot in real-time if attacks are occurring.

Behind the principles, there is a large variety of products, sometimes similar at all Hyperscalers, occasionally peculiar, to cover several mentioned areas of concern.
But the reader must consider two issues.

First of all, just recalling the previous chapter and the different styles of telco workload implementations, we need to consider that actual security controls could be highly vendor-specific, especially in the case of closed products like in approach 3. In this case, it is difficult for the final bearer of a security concern, the telco operator, to be 100% sure about security measures adopted by the technology vendor in the product design and deployment phases.

In addition, in a theoretical multi-cloud perspective, adopted to avoid single points of failure or Hyperscaler lock-in, one must consider that not all security tools are identical and seamless portability of a security framework from one Hyperscaler to another one is difficult. A technology vendor or an operator can use the best security features of each Hyperscaler, aiming at a coherent multi-cloud deployment, but 100% feature parity could be impossible.

Last but not least, though flexible and rich in features, the security products provided by Hyperscalers do not cover all the needs of telco workloads natively. In particular, they are not tuned for protecting the essence of 5G networks' control plane and the Service Based Interface over which network functions communicate, nor for protecting the legacy signaling networks. However, the responsibility for this component of the telco stack lies today entirely on the operators and not on the Hyperscalers.

SecurityGen mission is to shield the core of networks enabling the digital transformation of our society, and all the considerations above forced us to complete the stack of security tools and measures for 5G and legacy core networks with ad-hoc instruments.

6. SecurityGen vision for Telco workloads at Hyperscaler clouds

SecurityGen introduces ACE, the Artificial Cybersecurity Expert, and TSG, the Telecom Security Guard.

ACE addresses the inspection/audit and automation pillars of optimal Cloud security. ACE is a highly automated auditing tool for the 2G-5G control plane. ACE allows to define rich textbooks covering all possible cybersecurity threats affecting signaling networks: DoS against nodes and subscribers, frauds, disclosure of information, etc. Its power lies in two fundamental design values.

- Huge DB of inspection methods to test the security posture of the signaling networks. The DB allows to flexibly mount all types of attacks to 2G-5G core networks and check the networks' behavior.

- Automation framework, enabling to launch audit campaigns even several times per day without human intervention, thus freeing the operator from the burden of synchronizing network changes (sw releases, microservice components, topology, roaming partners) with inspection campaigns. With no human effort, you can ensure that any change in the network does not affect the robustness of the 2G-5G signaling core. Final reports of each test run are generated automatically and become readily available for security teams.

TSG is a robust combined Intrusion Detection (ID) and Intrusion Protection/Firewall (IP) System that embodies the principle of zero trust, inspection/audit/analysis, and automation too.

- Zero trust must also be reserved for protection measures and not only deployed in terms of identity and integrity of communications. Firewalls and border protection measures at STPs/DEAs/SEPPs are essential. Nevertheless, SecurityGen experience teaches that you cannot trust 100% these tools: border protection measures can be evaded by appropriately crafted messages. The TSG IDS component provides powerful analytics on all border signaling messages: no explicit attacks or potential threats can escape its lens, sharpened by a huge DB of attack signatures covering all mobile generations. Critical issues requiring immediate attention from security teams can be flagged in several ways and reported to SIEM.

- The TSG IPS is also a signaling recorder, storing signaling in its disks for months and allowing post-incident analysis or simply event analysis to improve the core network security posture.

- The highly integrated nature of the TSG IDS and TSG IPS components enables the one-click creation of IPS/FW rules from situations identified by the IDS. No complicated manual transfer, but instead simple, automated, and most of all error-free improvement of the behavior of the active FW protection.

With ACE and TSG, you can be sure that your network is 360-degree protected against attacks based on the use of SS7, Diameter, GTP, HTTP/2, and PFCP protocols, without adding any extra burden on security teams.

Reference:

1. **Towards a theory of ecosystems**- London Business School 2018 - Michael G. Jacobides | Carmelo Cennamo | Annabelle Gawer

2. **ENISA Documentation**https://www.enisa.europa.eu/publications/enisa-threatlandscape-report-for-5g-networks/

3. **CISA Documentation**https://www.cisa.gov/publication/5g-strategy

4. **3GPP on virtualization impacts:** 3GPP TR 33.848