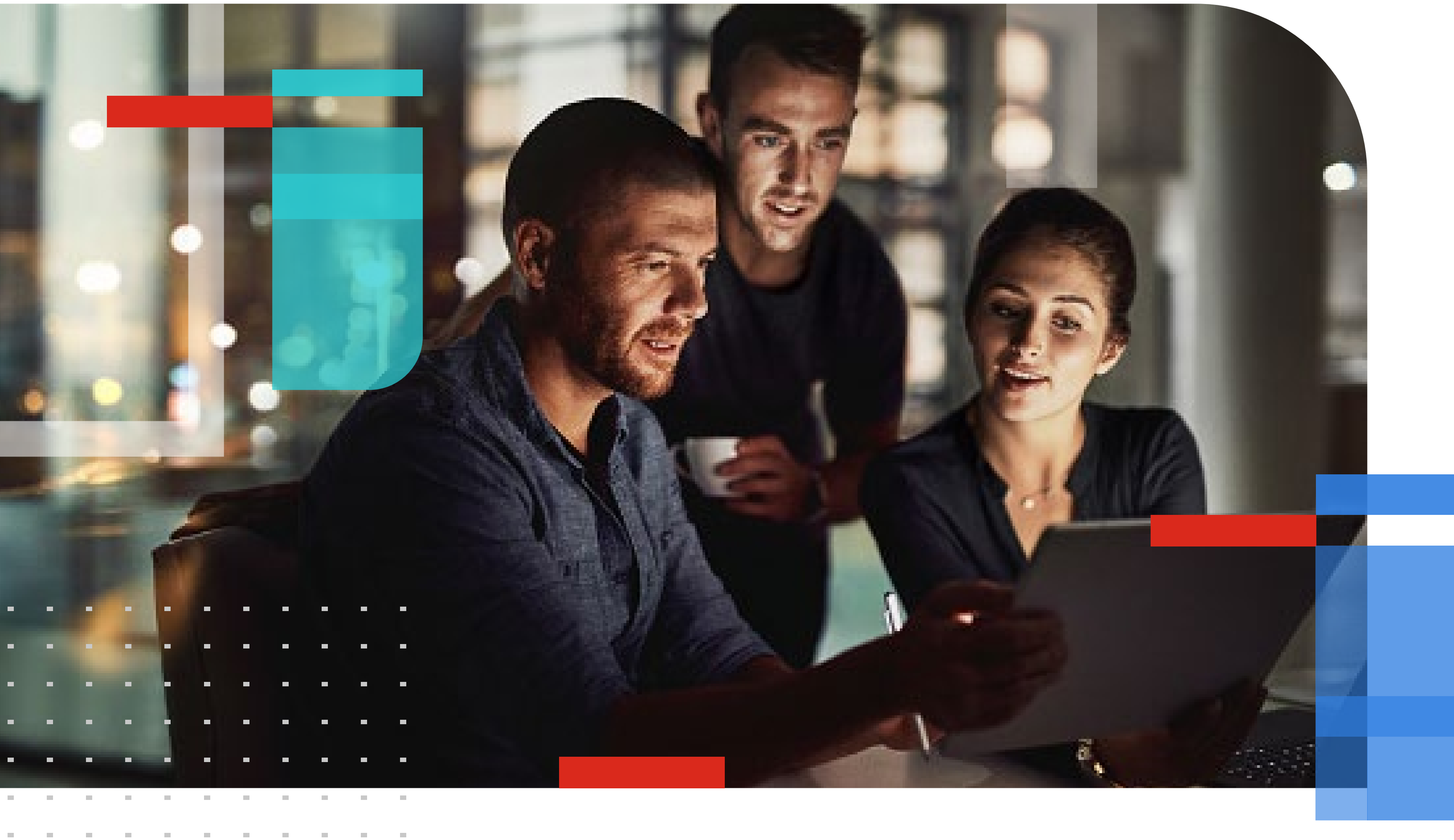
WHITE PAPER

Mobile Networks Domains and Their Cybersecurity Considerations



Cybersecurity is critical for mobile network operators (MNOs) and will play an important role in their evolution and growth in coming years. Mobile network operators must place increasing focus on protecting their networks, meeting both their own compliance requirements and those of their customers, safeguarding sensitive data, and providing high-value, secure services for enterprise verticals.

The inherent complexity of mobile network infrastructure and services creates many layers of vulnerability for MNOs. These include exposures stemming from backward compatibility, risks of human errors like misconfigurations, and the more common IT risks faced by every organization. With the increasing use of newer technologies such as the cloud, virtualization, and edge computing, the mobile network attack surface will continue to evolve and expand. It is therefore important for security to be implemented on all layers and over the breadth of the MNO network.

This document presents a layered view of security requirements across the MNO network, spanning all physical and logical domains, interconnections, exposure points, management, and orchestration.

2023 is shaping to be the year of telecoms hacks. All of the big 5G operators in the United States—Verizon, T-Mobile, AT&T, and Dish Network—have been involved in some kind of security incident already this year.[1]

MNO Domains and Cybersecurity Requirements

We can identify a certain set of common security requirements that are applicable to every layer of MNO domains and some specific requirements that are applicable to a specific layer on a specific domain. Such breakdown allows a holistic view of security requirements, which can later be mapped to relevant cybersecurity solutions, as shown in Figure 1.

Domains	RAN	Edge Cloud and Core Network		Roaming Security	Infrastructure Security	
Use Case	Centralized and distributed vRAN, cloud-RAN	MEC and edge cloud	Exposure security	With backwards compatibility	Physical	Virtualized
Use Case Description	▪ N3 content filtering ▪ SCTP FW anti-DDoS N2 ▪ Certificate-based authentication, encryption	▪ Container application security ▪ Container infra/ network security ▪ IDM, authentication, authorization ▪ Physical and virtualized infra security	▪ API security, schema validation ▪ Authorization, AF whitelisting ▪ Anti-DDoS, certificate-based authentication	▪ GTP IPUPS + SecGW + Anti-DDoS N9 ▪ PFCP Fw N4 ▪ SEPP and SEPP Protection Proxy N32 ▪ GTP Fw S8, S5 MAP/diameter Fw S6a, S6d ▪ MAP/diameter Fw S6a, S6d	▪ IDM, access control ▪ EDR ▪ Perimeter/ segmentation/ management/ API Fw	▪ Source code analysis ▪ Containerized firewalls east-west ▪ Ingress controller north-south ▪ Container orchestration platform hardening ▪ Container image and repository monitoring
Security Monitoring	Real-time log collection					
	Real-time log correlation					
	Incident response					

Figure 1: MNO domains and relevant cybersecurity requirements

All cybersecurity requirements in all domains should be based on four common principles:

1. **Defense in depth** to ensure that cybersecurity is integrated at all layers
2. **Zero trust** for continuous authentication and granular authorization
3. **Security by design** as recommended by the 3rd Generation Partnership Project's (3GPP) Technical Specification #33.501 and other standards
4. **Continuous event monitoring and incident response** based on the operators and business logic

Securing the Physical Infrastructure

The foundation of any modern network is based on the underlying physical infrastructure, regardless of its location, on-premises in a fully owned data center, at a collocated data center, or in a public or private cloud. To address the minimum requirements to protect underlying physical infrastructure across all domains:

- Deploy and manage perimeter firewalls.
- Implement a robust layer of authentication and authorization using technologies such as two-factor authentication and identity management.
- Protect web/API services, including authentication of requests, authorization, traffic-based protection, API schema validation, and anomaly detection.
- Apply hardware-based segmentation for tenants belonging to separate trust domains, especially in a cloud-based deployment. This ensures that two tenants from different trust domains do not share the same underlying physical infrastructure.
- Use an endpoint detection and response (EDR) tool to aggregate data on endpoints (including process execution, endpoint communication, and user logins), analyze data to discover anomalies and malicious activity, and record malicious activity data. This enables security teams to better investigate and respond to incidents. It also enables automated and manual actions to contain threats on the endpoint.
- Implement public key infrastructure (PKI), crucial for enabling critical security functions such as establishing an endpoint's identity, authentication, and authorization in multiple domains—such as radio access network (RAN), core, edge, and cloud.
- Integrate a hardware security module (HSM) with the 5G environment to provide and store strong cryptographic key and algorithm protection in tamper-resistant hardware. Like PKI, an HSM is applicable to both physical and virtual infrastructures.

Securing the Virtual Infrastructure

Mobile providers adopt virtualization technologies such as containerization to deploy flexible and scalable networks—especially in areas like multi-access edge computing (MEC) and core networks. The introduction of virtualization exposes the MNOs to multiple new attack vectors. In addition to the cybersecurity controls for physical infrastructure described, additional security controls need to be considered before deploying virtualized infrastructure:

- Strict role-based access control (RBAC) deployed on private image repositories to reduce an attacker's ability to access them.
- Security monitoring of container image repositories to prevent an attacker's ability to reach such registries, tamper with images, and create malicious images. These repositories need to be monitored continuously, including image updates.
- Continuous hardening of container orchestration platforms like Kubernetes, OpenShift, and Docker Swarm. These platforms introduce their own sets of vulnerabilities ranging from unauthorized access, privilege escalations, container escapes, lateral movements, and distributed denial-of-service (DDOS) attacks.
- Hardening the container orchestration platform to industry best practices to restrict attackers' ability to access, view, and execute unauthorized instructions to various components. A good starting point is to enforce the Center for Internet Security's (CIS) standards for target environments.

- Restricting access using stringent policies. A broad range of users and services need to access services hosted on containers, so it is critical to tie access to certain specific requirements:
  - Certificate-based authentication to enable access only to authorized identities
  - Granular authorization parameters using a combination of techniques (role-based, node-based, attribute-based, or webhooks), to restrict users to execute requests that are within their roles

$9.44M

The average cost of a data breach in the United States is **$9.44 million.**[2]

Securing Management and Orchestration

Operators often get attacked due to compromised management networks and inadequate security controls. Hence, it is critical to secure management and orchestration platforms and their connections to functional elements. To protect management networks from becoming vectors of attack on infrastructure, networks, and services:

- Harden management platforms including network function virtualization (NFV) platforms and the software-defined networking (SDN) controller
- Ensure that the management plane and services are not reachable from user plane networks
- Use the virtual infrastructure manager (VIM) to ensure segregation of network functions in different trust zones, via built-in logic or physical separation
- Encrypt configurations and other sensitive data
- Enforce the use of strong identity in combination with role-based access
- Enforce certificate-based authentication and authorization on management and orchestration APIs, applications, and supporting components
- Implement backup and recovery for the VNFs and platforms
- Use a trusted and secure time source
- Perform continuous inspection of API traffic, authentication, authorization, and anomaly detection

Securing Data Traffic

Data traffic is the most valuable asset within any network and the most coveted by threat actors. Data traffic can traverse multiple domains: RAN and transport, roaming, 5G-exposed interfaces, edge sites, and the internet/packet data network (PDN) edge. Below are some of the primary cybersecurity mechanisms that are needed in these domains:

RAN and transport. To secure communication and ensure confidentiality, integrity, and replay protection of traffic traversing the RAN:

- **Enable mutual authentication of various functional** elements such as Evolved Node B (eNB) and Next Generation Node B (gNB) base stations for 4G and 5G, and ensure rogue elements are not introduced to transmit untrusted data
- **Introduce a security gateway (SecGW/SEG)** to ensure end-to-end encryption of management and control plane traffic between the RAN, core, and orthogonal amplitude modulation (OAM) networks
- **Deploy intrusion prevention system (IPS) functionality** at the core demarcation points (N2 and N3) to detect protocol-based attacks, DDOS, or signaling storms

Roaming networks. These can be a major vector of attacks, as roaming interconnections can be used to exploit inherent weakness of roaming protocols for attacks on MNOs and their subscribers. The following minimal cybersecurity measures should be taken to ensure roaming cybersecurity:

- **Ensure route separation and infrastructure hiding** so the infrastructure should be transparent and not reachable for user and roaming traffic
- **Allow only expected services and protocols on roaming interfaces**, such as mobile application protocol (MAP), Diameter, and GPRS Tunneling Protocol (GTP)
- **Whitelist roaming peers** and their corresponding equipment on roaming firewalls or gateways
- **Enforce international mobile subscriber identity (IMSI) prefix filtering** and only allow requests limited to IMSI ranges per roaming agreements
- **Enable filtering and removal of informational elements** wherever required
- **Enforce roaming message security** by deploying specialized security equipment such as security edge protection proxy (SEPP) and firewalls for GTP, Diameter, and MAP
- **Ensure effectiveness of the above security measures** by penetration testing conducted by skilled personal in the areas of MAP/Diameter/GTP/API security testing

8.6%

Public companies lose an estimated **8.6% of their value** after a cyber breach.[3]

Core. Sharing data about network parameters like UE location, network usage/load, and traffic-steering rules enables MNOs to enhance services and even implement new revenue streams. It may also expose the MNO to attacks via untrusted application functions that may be part of a separate trust domain. As a result, adequate security needs to be in place to ensure that malicious requests are stopped before being passed on to the core network and prevent sensitive information from leaving the MNO's trust domains. To secure network exposure points:

- **Force certificate-based authentication** for external application functions (AFs)
- **Restrict requests** based on roles and trust level with OAuth 2.0-based authorization for authenticated AFs
- **Enforce rate limiting** to match the service-level agreements (SLAs) in place
- **Whitelist AFs** to ensure that only authorized functions are executed
- **Deploy API attack detection** to identify anomalous requests
- **Enforce API schema validation** to identify which requests are valid based on predefined properties
- **Implement anti-DDOS** to combat attempts to overwhelm the network
- **Deploy tools** to identify and block unwanted scan and bot traffic

Internet and PDN edges. These can be either in a centralized place or in an edge location such as an MEC. They potentially bring more attack vectors than any other domain, so they need to be adequately secured, regardless of location. Measures must be taken to:

- Stop volumetric DDOS and botnet attacks
- Protect against botnet attacks
- Detect and protect against automated and scan traffic
- Conceal the internal operator infrastructure
- Enforce content-based filtering (if required)
- Implement carrier-grade network address translation (CGNAT) to hide private address space

Cloud-native environments. Here it is important to enforce network policy in container orchestration solutions to ensure that only authorized pods can reach other pods and all other traffic is denied. Security policies need to be enforced on north-south traffic entering and exiting the clusters and east-west traffic to and from different pods within the container clusters.

Securing Services and Applications

The end goal of any MNO is to host high-value services and applications that can be monetized via enterprise and consumer consumption. In environments such as the 5G MEC, a number of these applications are managed by third parties and yet need access to the operator's assets. Commonly, these applications are in a cloud-native environment, which means that virtualization and containerization security are important considerations.

These factors position applications as a major potential attack vector. To limit the abilities of potential attackers at various stages, enforce cybersecurity throughout the application life cycle by:

- Performing code and software composition analysis (SCA) on all container images
- Monitoring and tracking access to, and vulnerabilities of, image repositories
- Tracking image vulnerabilities on deployed instances
- Hardening the container orchestration platform
- Enforcing certificate-based authentication
- Enforcing authorization controls (node-based, attribute-based, role-based, or webhooks)
- Implementing physical and logical separation of NFs in different trust zones
- Setting up an integrated certification authority (CA) for certificate signing
- Deploying an HSM for key generations and safe storage of keys

Conclusion

Sophisticated cyberattacks are escalating across every industry, and this is true for MNOs. A comprehensive security strategy is critical for MNOs as they work to deliver secure and reliable services to their customers. The complexity of their networks and services requires an integrated, multilayer, and multidomain approach to cybersecurity that will safeguard data, services, and value across all of their ecosystems.

The Fortinet Security Fabric provides an integrated and automated cybersecurity platform on which MNOs can build their entire cybersecurity infrastructure, capabilities, and services. It enables cybersecurity visibility, monitoring, enforcement, management, reporting, and orchestration across all domains, bolstering security and simplifying deployments and operations.

[1] Mike Dano, "Verizon, AT&T, T-Mobile, and Dish have all been targets of hacks this year," Light Reading, March 10, 2023.

[2] "Cost of a Data Breach 2022," IBM and Ponemon Institute, accessed March 28, 2023.

[3] Paul Bischoff, "How Data Breaches Affect Stock Market Share Prices," Comparitech, February 9, 2021.

FORTINET

www.fortinet.com

April 13, 2023 10:11 AM
2056604-0-0-EN