WHITE PAPER

Securing the Telco Management Plane

Cybersecurity Mechanisms and Fortinet Solutions

Executive Summary

Telecom providers' (Telco) networks, assets, and services have evolved to a complex, distributed, multivendor infrastructure, providing fixed and mobile communications, content, and value-added services to consumers and businesses. The nodes and network functions delivering these services must be configured, monitored, operated, updated, upgraded, scaled. These operations are performed through the management plane, which consists of an array of operational support systems (OSS) and business support systems (BSS) used by different teams within the organization.

The management plane is critical to the Telco's ability to deliver reliable and available customer services and generate revenues. Regulators worldwide are demanding that Telcos implement a set of security controls to achieve better management plane resilience (such as the U.K. Telecom Security Act-TSA).

This paper outlines key elements in securing the Telco management plane in a phased approach most suitable for its complexity and critical nature. Cybersecurity in the management plane is critical to the Telco's ability to meet regulatory demands. Integrated and automated within the Fortinet Security Fabric platform, Fortinet solutions deliver a cybersecurity foundation for basic, industry-standard, and advanced cybersecurity capabilities required to secure this environment.

The Security Challenge

- **Complexity:** 5G, 4G RAN and core, IMS, transport networks, content delivery networks (CDN), xTTH networks, and edge sites are only some of the domains that comprise the complex Telco environment. These all have corresponding multivendor OSS tools, which can integrate (or not) with a set of BSS tools. This results in complexity that is a challenge to effective security, with multivendor tools employing different software versions, operating systems, and security vulnerabilities, making it very hard to maintain a consistent security patching level.
- **Flat architectures:** Historically, the Telco management plane is an architecture that is flat by design, where most tools are in the same network or zone. This facilitates the ability of an attacker to move laterally within the plane, and any security issue has broad potential impact across the plane. For example, third parties and vendors providing remote support to element managers and tools located in the management plane represent a potential attack vector and risk from untrusted, external sources.
- **Lack of visibility:** Visibility of the management plane traffic and its behavior is often lacking. This hinders the ability to identify threats security issues and deploy proactive security measures.

These challenges create a large and porous attack surface that must be secured.

Each Telco network is unique (technologies and vendors used, scale, services, markets, resources), and so is its management plane and regulatory requirements. It is therefore important that we look at a phased framework to secure the Telcos' management plane based on specific requirements, building foundational cybersecurity that should be common to all Telcos.

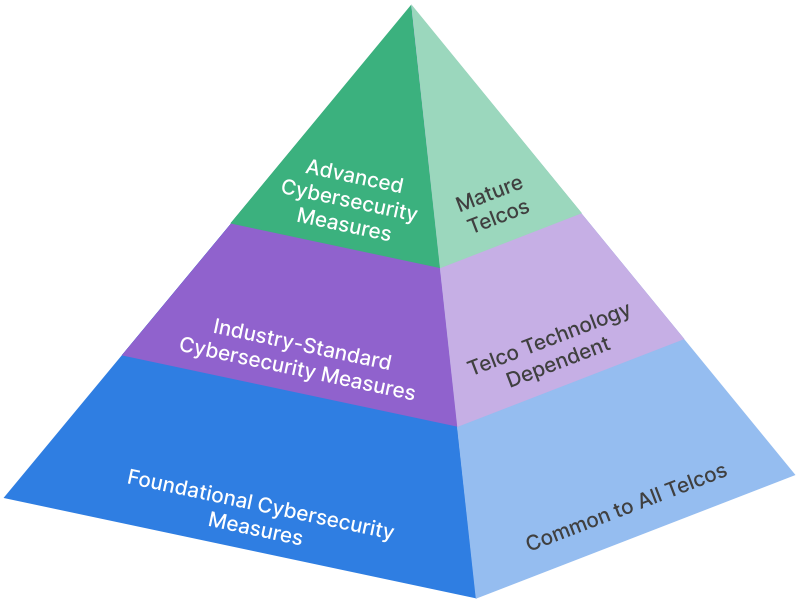

Figure 1: A phased approach for management plane security

The Basics of Foundational Cybersecurity Measures

This set of key measures and solutions should be implemented to build a solid cybersecurity foundation for the management plane and facilitate compliance with key cybersecurity regulations. These measures are based on zero-trust principles, defining the architecture of the management plane where identified elements, users, and other stakeholders are assigned to appropriate trust domains, with a specific trust level for each domain. The following table outlines some key measures that should be implemented at this level.

Measure	Trust zones definition (perimeter, segmentation, and segregation)	Implement strong credential policies	Implement trusted platforms for critical functions
Benefits	▪ Attack surface reduction ▪ Hamper lateral movement ▪ Create demilitarized zones for exposed trust domains ▪ Communication paths and privileged access enforcement	▪ Unique and secret trust zones credentials ▪ No hard-coded or default credentials ▪ Multi-factor authentication (MFA) ▪ Role based access control (RBAC) ▪ All login activity recorded	▪ Facilitates continuous security patching ▪ Facilitates continuous security posture assessment ▪ Security boundaries with no container or VM cut-throughs ▪ Endpoint protection facilitated ▪ Facilitates automation and exposed API security

Measure	All elements logging	Periodic testing and scanning	Implement asset management
Benefits	▪ Facilitates log correlation and enrichment ▪ Reduces detection and response time ▪ Logs should be stored on a hardened, separated system	▪ Discover shadow elements, functions, and interfaces ▪ Improve availability and performance of interfaces and APIs ▪ Identify vulnerabilities and risks	▪ Facilitates continuous installed asset visibility ▪ Facilitates network access control

Measure	Risk assessment
Benefits	▪ Provides vulnerability analysis and risk score ▪ Help decide on acceptable risks ▪ Helps prioritize actions and investments based on assessment

The following table provides a breakdown of the Fortinet products that support implementing the above key measures.

	Trust zones	Strong credential policies	Trusted platforms	Logging	Testing and scanning	Asset mgmt.	Risk assessment
FortiGate	●		●				
FortiWeb	●		●				
FortiPAM		●					
FortiAuthenticator		●					
FortiToken		●					
FortiEDR			●				
FortiSIEM				●		●	●
FortiSOAR						●	●
FortiRecon					●		
FortiMonitor					●		
FortiSASE		●					

Technology Specific to Industry-Standard Cybersecurity Measures

While the foundational cybersecurity measures outlined are generic and should be applied by any type of Telco organization, industry-standard measures deal with specific technologies and use cases. Therefore, they may be relevant in different ways to different Telcos based on their use of specific technologies and ecosystems. The following table outlines key measures that should be implemented at this level and those mentioned before.

Measure	Secure private cloud	Secure public cloud	Advanced third-party security
Benefits	▪ Private cloud as a trusted platform ▪ Images scanned to detect and mitigate vulnerabilities and attacks ▪ Protection against application-specific attacks ▪ Secured cloud tenants ▪ Application secrets are protected ▪ Facilitates API automation and exposure security	▪ Public cloud as a trusted platform ▪ Exposed interfaces are protected ▪ Images scanned to detect and mitigate vulnerabilities and attacks ▪ Public cloud tenants are secured ▪ Protection against application-specific attacks ▪ Zero-trust principles applied to data and applications	▪ Secured third-party access to Telco networks and assets ▪ Zero-trust access enforces trust domains and trust levels for third parties ▪ External files scanned to detect and mitigate vulnerabilities and attacks ▪ Third-party sessions are recorded to facilitate auditing and analysis

Measure	Traffic monitoring	Security operations	Advanced vulnerability management
Benefits	▪ Enforced anomalies and attack detection ▪ Facilitates misconfiguration discovery ▪ Detection to mitigation time is shortened	▪ Gathering, triage, analysis, and correlation of logs facilitate SOC workload ▪ AI-based tools aid and greater automation to increase SOC analysts' efficiency and effectiveness ▪ Asset discovery is facilitated, and possible conflict resolution is shortened ▪ Reduction of false positives ▪ Shortened discovery to mitigation with cybersecurity enforcement points integration and automation	▪ Vulnerabilities disclosure from suppliers and vendors ▪ Assets inventory correlation against known vulnerabilities (CVE) ▪ Regular schedule of vulnerability patching and virtual patching

The following table provides a breakdown of the Fortinet products supporting the implementation of the above measures.

	Secure private cloud	Secure public cloud	Advanced third-party security	Security operations	Traffic monitoring	Advanced vulnerability management
FortiGate	●	●				
FortiWeb	●	●				
FortiPAM			●			
FortiAuthenticator			●			
FortiToken			●			
FortiEDR	●	●				
FortiSIEM				●	●	
FortiSOAR				●		●
FortiRecon			●			
FortiNDR					●	
FortiCNP	●	●				
FortiSASE			●			

Mature Telcos with Advanced Cybersecurity Measures

This added group of measures enhances and provides further security control and protection that may not be common or required by all operators to secure their management plane. These measures may also be required to comply with specific regulations and operational environments specific to Telcos. The following table outlines some of the key measures recommended at this level.

Measure	Deception	Enhances zero-trust network access (ZTNA)	Data loss protection (DLP)
Benefits	▪ Facilitates early lateral movement detection ▪ Enables early threat mitigation ▪ Provides threat intelligence to enhance security posture and readiness ▪ Shortened mitigation times with cybersecurity enforcement points integration and automation	▪ Continuous and dynamic trust level validation and enforcement ▪ Least-privileged access rights enforced everywhere and all the time ▪ Real-time and accurate access enforcement via agent deployment	▪ Protects against insider data exfiltration ▪ Supports compliance with data protection regulations

Measure	Cybersecurity automation	CI/CD pipeline security integration
Benefits	▪ Improve management plane cybersecurity efficiency, time to discover and mitigate, and reduce potential damage ▪ Deploy security orchestration, automation, and response (SOAR) ▪ Implement playbooks and workflows to automate cybersecurity responses to events in the management plane ▪ Use AI tools integrated with SOAR to increase efficiency and response	▪ Applications and workloads are secured by design ▪ Increase in product life-cycle security

The following table provides a breakdown of the Fortinet products supporting the implementation of the above measures.

	Deception	Enhanced ZTNA	DLP	Cybersecurity automation	CI/CD pipeline security integration
FortiGate		●	●		
FortiWeb			●		
FortiPAM					
FortiEDR		●			
FortiSOAR				●	
FortiClient		●			
FortiClient EMS		●			
FortiDevSec					●
FortiDeceptor	●				
FortiSASE		●	●		

Conclusion

Securing the Telco management plane is critical to their ability to deliver service availability and reliability and meet relevant regulatory requirements.

Fortinet enables Telcos to approach and implement cybersecurity for the management plane efficiently and effectively by:

- Providing the tools and expertise to design and implement much-needed security visibility and enforcement based on the Fortinet Security Fabric platform
- Enabling a phased implementation based on specific Telco requirements (technology, architecture, scale, regulations)
- Offering flexibility with native solutions integration, automations, and flexible licensing

September 16, 2024 3:39 PM / 2853522-0-0-EN