WHITEPAPER

How Three-in-One Cybersecurity Can Drive Value for Your MNO Business

Protect critical services, drive monetization and support key compliance requirements with a centralized, automated cybersecurity platform fit for the 5G age.

Published by

MOBILE WORLD LIVE

In partnership with

FORTINET®

Executive Summary

Mobile network operators (MNOs) are well aware of the need for comprehensive cybersecurity capabilities. They understand that they run complex, interconnected and highly distributed infrastructure which provides an enormous attack surface for threat actors to target. They know too that this surface is expanding ever further with 5G, and that they also need to protect legacy networks. Yet up until now, cybersecurity has been an investment framed in terms of mitigating risk and protecting critical networks, assets, and services. That's understandable at a time when telcos from Sydney to Kyiv are reeling from serious security breaches.

But it's not the whole story.

In fact, at a time when MNOs are looking to trim costs, drive growth and improve return on investment (RoI), cybersecurity should also be viewed as a powerful business enabler. It can be a force multiplier for establishing enterprise trust and service consumption. And more directly, it offers the opportunity to drive revenue by delivering security services to consumer and business customers. At the same time, a powerful, comprehensive cybersecurity platform is critical to helping MNOs meet an increasingly rigorous set of critical national infrastructure (CNI) regulations; from New Delhi to New York.

This paper will explore the challenges facing MNOs as they transition to a new 5G era and how centralized, automated security capabilities can do more than mitigate cyber-threats. They can drive value across the business—from monetization to compliance.

The Story so Far

MNOs are navigating an intensely challenging period. While 5G offers much, it has so far failed to deliver on its much-hyped, transformative potential to drive multibillion-dollar growth. At the same time, regulators across the globe are placing ever more onerous requirements on MNOs. This itself is partly a response to surging threat levels and the growing criticality of communications infrastructure to the global economy. In this context, MNOs are faced with three key challenges:

1) Threats, Vulnerabilities, and Operational Headaches

MNOs have always been an attractive target for hackers due to their sizeable revenue, the critical role they play in supporting the digital economy, and the large volumes of personal data they process. But the journey to delivering on the promise of 5G is paved with even greater cyber risk. This includes:

IT vulnerabilities: Because MNOs are rapidly adopting IT technologies to support this evolution – including cloud computing, virtualization technologies and API-driven communications – they are exposed to the same types of cyber-threats and vulnerabilities as regular enterprises. There was a record number of vulnerabilities (CVEs) reported in 2022, and a new record was set in 2023. Threat actors are past masters at finding ways to exploit these software flaws, often using social engineering techniques like spear-phishing to do so. This could ultimately lead to unauthorized access, data theft, ransomware, and/or complete system/application compromise.

Extensive supply chains and heterogeneous technology: As a result of 5G-related digital transformation – which also includes multi-access edge computing (MEC) – MNOs are more exposed than ever. Multi-vendor, multi-layer, and multi-partner supply chains have increased the attack surface further, providing multiple points of potential compromise across large, distributed environments. These might span physical, virtual, or cloud-native systems across MNO-owned data centers or public and private hybrid platforms.

Backwards compatibility: These challenges are multiplied by the need to ensure backwards compatibility between 5G and previous generations, as well as operators yet to transition to the newest technologies. This further expands the potential attack surface for threat actors, who could exploit vulnerabilities in legacy technology to bypass the security controls of modern networks. For example, although 5G standalone roaming features built-in controls to enhance trust between roaming MNOs and intermediaries in the roaming control plane, legacy tech does not. So attackers could still target 5G MNOs with 4G roaming attacks.

Poor security practice: Misconfiguration and failure to align with industry best practices is another common risk. It's a risk that's amplified by the greater complexity of 5G network architectures and distributed environments and the expanded size of the MNO attack surface. Many organizations don't have access to enough skilled professionals trained in how to manage, secure, and correctly configure new 5G technologies.

Skills shortages: MNOs have been reducing staff numbers to cut costs, making it even more challenging to handle surging risk and complexity. That's despite industry-wide skills shortages in cybersecurity which have led to a shortfall of four million professionals globally. MNOs arguably need more, not fewer, skilled security professionals to help with the transition to 5G. instead, they are trying to do more with less.

2) Growth, Monetization and Return on Investment

By 2025, 5G networks are predicted by the GSMA to cover one-third of the world's population, or around 1.2 billion connections. Yet after investing heavily in infrastructure, as well as spectrum licenses, and cloud and edge computing, an expected revenue bonanza has yet to materialize. Many MNOs are now looking to reduce costs. AT&T's capital expenses (capex) are predicted to be $1 billion lower in the second half of 2023 than the first six months of the year.

However, these cost-reducing measures could expand the attack surface further and expose MNOs to new security risks. They include:

RAN sharing: RAN infrastructure is a major expense for MNOs especially in more remote and sparsely populated areas. Sharing this infrastructure can help them reduce total cost of ownership (TCO), but also increases privacy and security risks.

Neutral hosting and tower/fiber companies: These represent another useful way for MNOs to reduce capital and operational costs. By getting a third party to invest in cell towers, real estate, and fiber-optic networks the MNO has more capital to spend on other activities like 5G service rollouts. But sharing this infrastructure with partners and competitors could expose MNOs to an elevated risk of breaches.

At the same time, MNOs are struggling to justify more investment, and instead want to drive more return on their significant outlay on 5G to date. To do so, they must steer away from providing pure-play connectivity. Although mobile data traffic is set to grow 28% year-on-year in 2023 and 24% in 2024, analysts believe that only new applications and services will unlock double-digit annual growth. The ultra-fast, low-latency connectivity of 5G holds huge potential for monetization. But security must play a critical role here too. Consider the following:

Network exposure initiatives: Service exposure within the network domain is about making network capabilities and key data/telemetry available to developers, enterprises and other third parties. Industry initiatives like the GSMA Open Gateway are helping to accelerate such moves by supporting standardized consumption of network and user information APIs for application developers. That in turn will spur development of a diverse range applications to harness the power of 5G networks across multiple verticals – from healthcare to entertainment.

Network slicing initiatives: 5G makes it easier to devote a full network slice or a simpler DNN/APN to a large enterprise or a specific use case, generating new revenues while optimizing cost structure. Cybersecurity is a value-add service that can be offered in a dedicated network slice. At the same time, having multiple tenants/slices in the network requires additional layers of security to isolate and protect them.

But for such monetization efforts to succeed, developers must trust that these APIs are secure and compliant for their end users, while MNOs must also mitigate the risk of untrusted API consumers (applications, enterprises and partners) The challenge is that APIs are a common target for threat actors. A March 2023 report claimed that API attacks increased 400% in the previous six months. Weak authentication and misconfiguration are common problems, although there are many potential security risks to mitigate with secure-by-design approaches and the right security controls. The traditional controls of encryption and authentication are not sufficient to provide MNOs with the assurance that API consumers can be trusted. Additional layers are needed.

3) Proliferating Compliance Mandates

As communications technology becomes critically important to countries, their societies and economies, governments are stepping in to ensure the organizations that run critical infrastructure do so in a secure and resilient manner. The idea is broadly to reduce the chances of serious service outage or data loss, which could have a major downstream impact on the businesses and consumers depending on such services. Ensuring compliance with these regulations is not only a legal requirement in various jurisdictions, it is critical to winning the trust of enterprise customers as MNOs look to expand their value-add services beyond pure-play connectivity.

Among the laws that have appeared over recent years are:

UK – Telecoms Security Act (TSA): Demands MNOs deploy and enhance a range of security controls in their own and supplier environments, to proactively mitigate the risk of compromise.

EU – NIS2 directive: Updated directive for "operators of essential services" featuring a new minimum set of baseline security requirements.

Canada – Bill C-26: Requires operators of critical cyber systems to implement a cybersecurity program, mitigate supplier threats, and notify regulators about incidents.

How Three-in-one Security Can Solve These Challenges

Against this challenging backdrop, MNOs need a natively automated and integrated cybersecurity platform that spans their entire environment, from the core to the edge and the endpoint to the SOC.

Only a cybersecurity platform-based approach can support service providers' technological, architectural, and service complexity – and deliver effective and efficient cybersecurity protection, monetization, and compliance. Unlike point solutions, a cybersecurity platform integrates vendor-specific and third-party capabilities, providing greater automation, visibility and collaboration across endpoints, networks, cloud, applications, and services. A mature cybersecurity platform will reduce operational costs, drive operational efficiency and optimization, improve overall cybersecurity, and help maintain business continuity.

The scale and complexity of MNOs demands a platform with carrier-grade performance, native multitenant capabilities, ease of integration via rich set of APIs and protocols, and a powerful set of visibility, automation, and orchestration capabilities.

A platform approach offers several benefits, beginning with consolidated coverage that ensures MNOs have fewer cybersecurity vendors to manage. It also features natively integrated capabilities that share information such as events, threats, and telemetry from different parts of the network. This enhances MNO visibility and control. By adding a high degree of automation, such a platform will be able to reduce human error, accelerate threat response, improve outcomes, and free staff to work on higher value tasks.

Above all, a three-in-one cybersecurity platform should:

- Enable protection, detection and response to threats and vulnerabilities
- Drive monetization directly and indirectly by building enterprise customer trust, protecting network exposure and delivering revenue-generating security services
- Support compliance requirements within the MNO and for enterprise customers
- Make all of the above possible with automation and security operation (SecOps) capabilities

Let's consider how this three-in-one approach would work:

1) Protection

MNOs need to empower enterprise customers to embrace new technologies and ways of working—from cloud and virtualized servers to application-centric DevOps and AI. They need to support new architectures such as RAN sharing, neutral hosting and highly distributed 5G environments. And they must strive to deliver on the promise of new services and use cases—from MEC and IoT to private 5G networks and network slicing—not to mention fresh network exposure initiatives. To make this a reality, they need a cybersecurity platform that delivers threat protection, detection and response with carrier-grade scalability, performance, and availability across a large number of sites and devices. It must support flexible deployment across physical, virtual, containerized, and multi-tenant architectures. And add value across a large spread of potential use cases in industry verticals as diverse as gaming, healthcare, and transportation – as well as MNOs' internal networks and service security.

2) Monetization

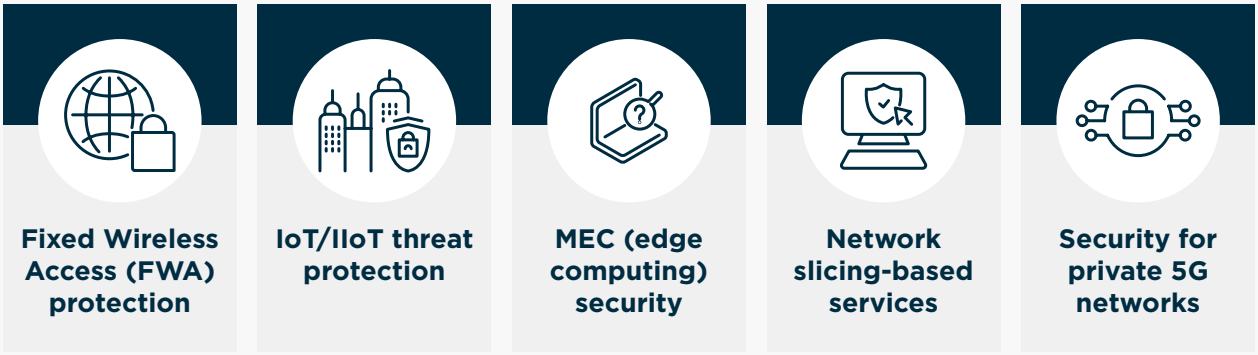
A GSMA Intelligence survey reveals that mobile operators consider security investment as their top operational priority to achieving long-term enterprise revenue goals. MNOs should therefore leverage a cybersecurity platform that can deliver indirect and direct growth by:

- Delivering value-add services direct to end-customers:

Consumers could benefit from a range of services including premium "digital wellness" subscriptions designed to encourage a more responsible and healthy relationship with technology. Such packages could include advanced parental controls, anti-botnet/anti-malware services, screen time tracking, and content filtering. These services can also open the door to more monetization opportunities by providing user insight to help build more personalized and relevant future offerings.

These cybersecurity services can be integrated into a network slicing offering or can be delivered as a Service (Security aaS) in the form of SASE (Secure Access Service Edge) on top of a regular connectivity offering.

Enterprises could benefit from services including:



Delivering enhanced security which indirectly drives enterprise trust and therefore greater consumption of 5G services, such as:

Security at the edge, where heterogenous operational technologies represent a growing risk

Security reporting, in order to support customer compliance efforts and enhance transparency

Multi-tenant separation – especially in RAN sharing and neutral host environments

Security service level agreements (SLAs) to drive assurance and trust

API protection through authentication, encryption and web application firewalls

3) Compliance

Cybersecurity is a fundamental pillar of any compliance strategy. And although compliance with external regulations does not guarantee an organization will be 100% breach-proof, it is both a legal requirement and an important step to mitigate business risk. Yet MNOs must navigate an increasingly challenging regulatory landscape. According to Verizon, compliance concerns are among the top-two most common barriers to 5G adoption. A cybersecurity platform should therefore provide MNOs with the confidence that they are adhering to local laws and industry best practices, and provide similar assurances to enterprise customers where relevant.

The EU's NIS2 directive is typical of such regulations. It's designed to improve the bloc's capacity to prepare for and respond to cyber-threats through new baseline security requirements for "essential entities" and tougher penalties for non-compliance.

These requirements are:

- Risk management and information security policies
- Incident prevention, detection, and response
- Business continuity and crisis management
- Supply chain security
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- Security risk management assessments
- Policies and procedures on use of strong encryption

A full-featured, integrated platform would therefore need to include capabilities such as:

- Digital risk management (eg SIEM, SOAR and GenAI-based SecOps assistants)
- Threat detection and response spanning reporting systems across the attack surface
- A resilient, high availability architecture and rapid disaster recovery
- Comprehensive visibility into cloud and CI/CD pipelines for code vulnerability management
- Access controls, network segmentation, API security, deep traffic inspection, and support for DevSecOps, vulnerability sharing and data protection
- Asset management, risk profiling and security monitoring, auditing, and testing
- Protection of API communications, and secured control, management and user plane traffic spanning the Core, RAN, Roaming and Datacenter environments

Such considerations should provide an idea of the wide variety of integrated capabilities MNOs require to meet today's often rigorous compliance mandates.

How Fortinet Can Help

Investment in network and service evolution requires a long-term strategic approach, and so too does cybersecurity. Such is the heterogeneity, complexity, and distributed nature of MNO environments that a heavily automated and tightly integrated platform is essential.

Fortinet provides this through its Fortinet Security Fabric: a comprehensive cybersecurity mesh platform built on the pillars of AI-based protection, app security, secure networking, endpoint protection and SecOps capabilities. The Fortinet Security Fabric offers MNOs everything they need to securely manage public and private 5G —from the RAN to the core, and beyond to the edge, applications, public/private clouds and third parties. It is security built from the ground up to deliver threat protection, detection and response and policy enforcement across the entire attack surface. AI-powered analytics and intelligent automation close security gaps, reduce complexity and accelerate positive outcomes.

With this architecture in place, MNOs can start to harness cybersecurity as a business enabler—not just for protection against critical threats, but to drive important monetization efforts and support mandatory compliance requirements. This kind of three-in-one cybersecurity can help MNOs finally deliver on the promise of 5G and beyond and chart their own path to sustainable growth at a challenging time for global businesses.

Founded more than 20 years ago in Sunnyvale, California, Fortinet continues to be a driving force in the evolution of cybersecurity and the convergence of networking and security. Securing people, devices, and data everywhere is our mission. To that end, our portfolio of over 50 enterprise-grade products is the largest integrated offering available, delivering proven cybersecurity everywhere you need it. More than 730,000 customers trust Fortinet solutions, which are among the most deployed, most patented, and most validated in the industry.

Find out more at www.fortinet.com

Mobile World Live is the premier destination for news, insight and intelligence for the global mobile industry. Armed with a dedicated team of experienced reporters from around the world, we are the industry's most trusted media outlet for breaking news, special features, investigative reporting, and expert analysis of today's biggest stories.

We are firmly committed to delivering accurate, quality journalism to our readers through news articles, video broadcasts, live and digital events, and more. Our engaged audience of mobile, tech and telecom professionals, including C-suite executives, business decision makers and influencers depend on the unrivalled content and analysis Mobile World Live provides to make informed business decisions every day.

Since 2016, Mobile World Live has also had a team of in-house media and marketing experts who work directly with our brand partners to produce bespoke content and deliver it to our audience in strategic yet innovative ways. Our portfolio of custom work - including whitepapers, webinars, live studio interviews, case studies, industry surveys and more – leverage the same level of industry knowledge and perspective that propels our newsroom.

Mobile World Live is published by, but editorially independent from, the GSMA, producing Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and home to GSMA event keynote presentations.

Find out more at www.mobileworldlive.com

Disclaimer: The views and opinions expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the GSMA or its subsidiaries.