SOLUTION BRIEF

Beyond Connectivity: Mobile Network Operators' Cybersecurity Monetization for Consumer and Enterprise Markets

Monetization of mobile networks using data-centric revenue models (dumb-pipe models) has always proved challenging. Global mobile data traffic almost doubles every two years,[1] but its revenues are constantly decreasing.[2] Mobile network operators (MNOs) continue investing in significant network infrastructure, spectrum licenses, telco cloud, and edge computing.

Operators must steer away from the "give more, get less" trap of providing pure-play connectivity via services and applications monetization on top of pure connectivity for the consumer and enterprise markets.

Enterprises are expected to play a significant role in driving growth in 5G due to the various capabilities and benefits that 5G networks offer. The potential for monetization is immense. 5G networks provide ultra-fast, low-latency connectivity, which enterprises can leverage for many use cases.

However, as we delve into the realm of monetizing 5G networks, it is crucial to address network security as a paramount enterprise concern. The ecosystems and use cases that are driven by 5G can only be fully consumed by enterprises and monetized only if these concerns are addressed:

- Increased attack surface: The sheer volume of connected (and many headless) devices and applications greatly expands the attack surface, making networks more susceptible to cyberthreats.
- Distributed edge computing: Edge computing in 5G allows data processing closer to end-users but also demands robust security at these distributed points.
- Greater network and resource exposure: To partners and third parties to deliver new capabilities and services.
- Zero-trust architecture: Implementing a zero-trust architecture is crucial to authenticate and authorize users and devices, but it requires comprehensive security measures.
- Data privacy and compliance: Ensuring compliance with regulations like GDPR or the NIS2 Directive, in addition to industry-specific regulations, is imperative.
- Supply chain vulnerabilities: The 5G supply chain is global and complex, making it susceptible to hardware and software vulnerabilities.

These challenges concern enterprises of all sizes and business verticals. Failure to address them will hurt mobile network operators' ability to fully monetize their networks and services.

Cybersecurity is a positive network and service monetization factor for MNOs:

- Indirectly by facilitating network and service adoption by enterprises
- Directly by delivering cybersecurity value-added services to consumers and enterprises

Fortinet enables MNOs to deploy cybersecurity services to drive network and service monetization to consumers and enterprises using security elements deployed on the mobile user-plane. These can provide value-added cybersecurity services or secure and protect service platforms and ecosystems. Security by design is the fundamental enabler platform upon which all 5G monetization use cases can be built.

The following paragraphs provide some examples of cybersecurity as a monetization enabler by Fortinet.

Monetization with Digital Wellness for Consumers

Digital wellness services promote healthy technology use in the consumer market. Mobile operators can offer premium digital wellness subscription services to their customers, including features like advanced parental controls, advanced security like anti-botnet or anti-malware services, screen time tracking, content filtering and monitoring services that allow parents to control and monitor their children's online activities.

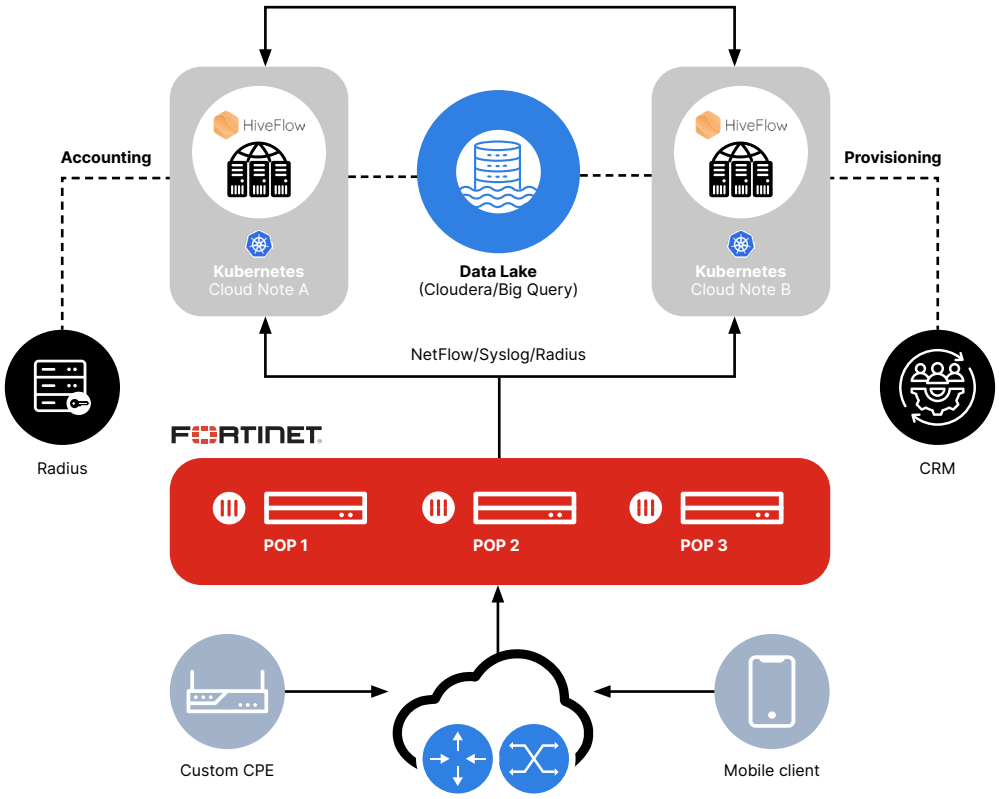

Figure 1: Fortinet and Nethive Digital Wellness solution architecture

Monetization extends beyond the mobile users' digital wellness subscription fee. The transparency into user traffic presents an invaluable avenue for amassing data for business analytics. This empowers the operator to discern the predominant digital behaviors exhibited by its clientele, thus affording insights into the types of services and analogous products that align with their preferences.

Monetization with Cybersecurity Services for the Enterprise Market

A wide range of cybersecurity services is applicable to the enterprise segment to support and generate service monetization in both 4G and 5G. These can be generic cybersecurity services or ones tailored to industry, enterprise, use case, or slice.

The following paragraphs provide some examples as enabled by Fortinet.

IoT Cybersecurity Services

Many connections, low bandwidth, and low revenue and margins characterize most IoT connectivity services. Any additional service and capability that can contribute to IoT monetization is important.

Connected IoT devices also represent a security concern for enterprises as they are exposed to physical and cyberattacks and can be used as part of massive botnets to attack the enterprise and the overall IoT ecosystem.

Fortinet FortiGate NGFWs provide a platform that allows MNOs to offer a secure IoT service for enterprises to protect the IoT devices themselves and their data, ensure the integrity of connected devices, and prevent unauthorized access. These security services can also be applied to protect the enterprise IoT platform and applications from being attacked by IoT botnets and compromised IoT.

Read the "Cybersecurity Considerations in IoT Ecosystems and Services" white paper for more detailed information.

Cybersecurity for Private Networks

Ensuring the security of a private mobile network (PMN) should be considered critical for the enterprise and the MNO. PMNs are not entirely isolated (only in rare cases). They are connected directly to the enterprise network (and from there are exposed to any external network connectivity, such as the internet), the internet, and partners and third parties. PMNs in industrial environments can also impact industrial security when no additional cybersecurity is included.

Fortinet enables MNOs to embed security solutions and services to protect any PMN, 4G and 5G, and maintain the overall enterprise security posture.

Read the "Cybersecurity Considerations in Industrial 5G Environments" white paper for more detailed information.

Network Slicing–Based Cybersecurity Services

5G network slicing provides independent logical networks over a common public or private mobile network, where each slice may have different characteristics, configurations, and policies to meet a variety of use cases and service level agreements (SLAs). Network slicing should be a premium, high-value, revenue-generating service targeting enterprises looking to implement use cases requiring specific mobile connectivity privacy and SLAs.

Providing cybersecurity services as part of slice-unique resources, configuration, services, and SLA facilitates the adoption of network slicing services by enterprises and will serve as an additional source of revenue and differentiation for the mobile provider.

Read the "Value-Add, Slice-Based Cybersecurity Services" point of view paper to learn more about how Fortinet delivers slice-based cybersecurity services.

Cybersecurity Services in Mobile Edge Compute

Mobile edge computing or multiaccess edge computing (MEC) enables data processing near the data source to minimize latency, enhance privacy, reduce traffic-related costs, and enable new use cases. MNOs are investing in building edge compute sites, platforms, partnerships, and value ecosystems for enterprises to consume.

For enterprises looking to enable innovation via the use of MEC sites and services, some security considerations will facilitate enterprise consumption and revenue generation:

- MECs are multi-tenant environments where separation and isolation are required.
- MEC sites are connected to the internet and other public networks.
- MEC sites can be accessed by partners and third parties.
- Cybersecurity visibility and compliance must be maintained within the MEC.

Fortinet enables MNOs and MEC providers with cybersecurity visibility, controls, and reporting to meet the above requirements and facilitate enterprise MEC consumption. Some or all these cybersecurity capabilities can be delivered as revenue-generating value-added services:

- Securing the connectivity between the mobile user plane and the MEC user plane.
- Provide secure SD-WAN connectivity to other MEC platforms and locations.
- Security microsegmentation for tenant, slice, and application isolation.
- Securing MEC network and resources access and usage.
- Web application and API protection (WAAP) to ensure the MEC's applications and APIs.
- IoT security services are required for IoT platform components residing in the MEC.

Conclusions

Beyond consumer-facing 5G services, the 5G promise and monetization have fallen short of the world-changing, billions-dollar hopes around industries' digital transformation. The path forward is going beyond just B2C and into B2B and B2B2X models and services where 5G facilitates new services and use cases for enterprise verticals and consumers. There is a growing understanding that a mobile provider's bigger value lies in helping the enterprise solve business problems via the evolution of 5G from a network into a platform encompassing connectivity, services, applications, and use cases.

Cybersecurity can be an accelerator and differentiator for MNOs to monetize their networks and services further. Fortinet enables MNOs to incorporate a rich set of cybersecurity value-add services to drive monetization in the consumer and enterprise markets.

November 4, 2023 7:42 PM

2403970-0-0-EN