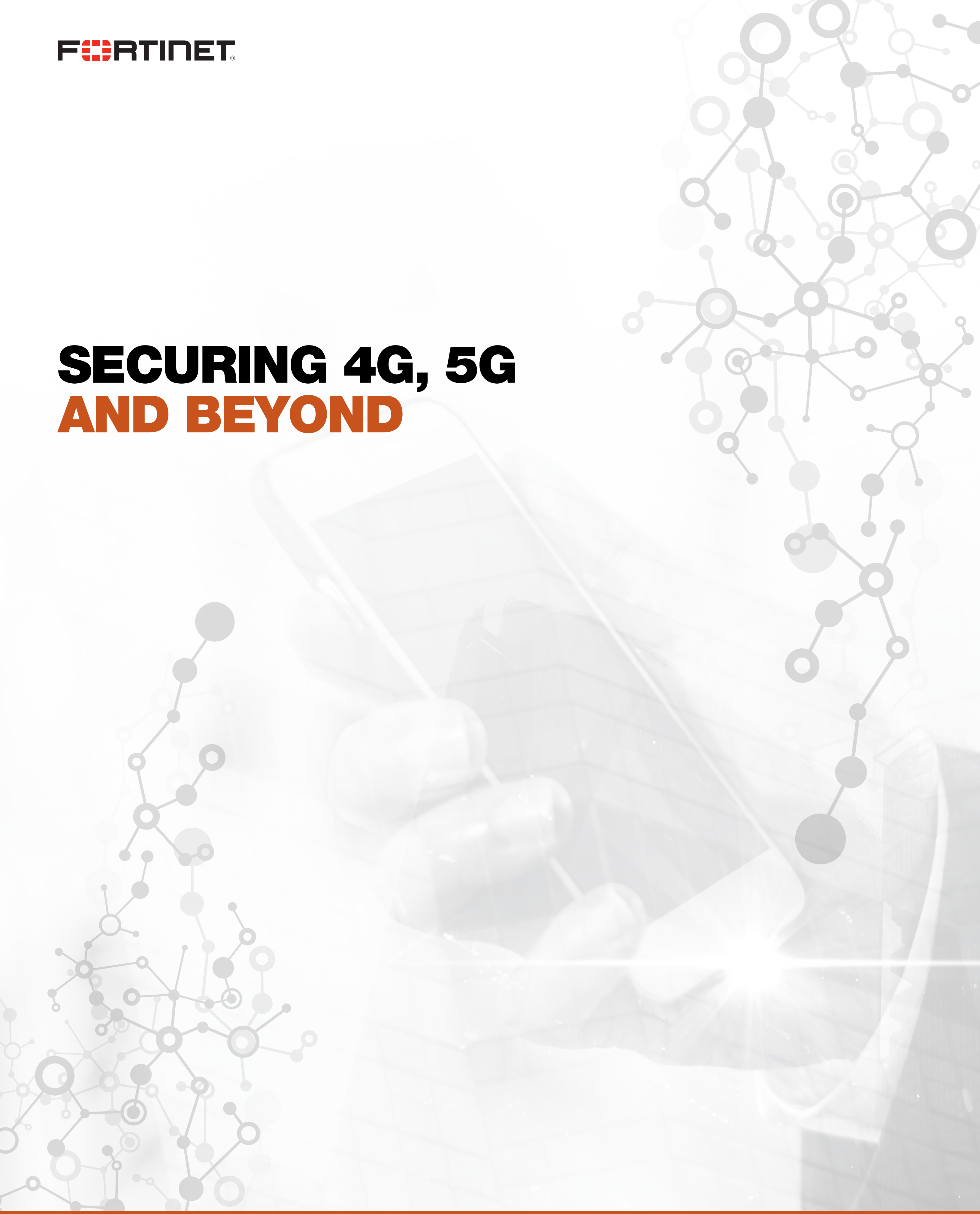
FORTINET

SECURING 4G, 5G AND BEYOND



WHITE PAPER

SECURING THE MIGRATION TO 5G AND BEYOND

TABLE OF CONTENTS

SECURING THE INVISIBLE NETWORK

The ideal communications network is invisible to the user. In the same way that we no longer worry about the reliability, performance or security of electrical circuits when switching on a light, we have always strived for that same instant access to our data, applications and services, wherever and whenever we choose. With 5G, this long-sought yet elusive goal finally promises to become a reality, ushering in new possibilities and opportunities, the extent of which seems limited only by our imagination.

The advent of 5G will extend ‘digital connectedness’ to almost every facet of our lives. In many of the somewhat futuristic-sounding new use cases, such as autonomous vehicles, virtual and augmented reality, smart cities, and the long-hyped Internet of Things (IoT), 5G has been the missing puzzle piece. For years now, the mobile interconnection of all these things has seemed inevitable, yet the massive density of connections, all with adequate speed, latency and related services, had so far remained unachievable in all but limited proof-of-concept testing.

But with the coming orders-of-magnitude advances in bandwidth, connection and use case possibilities, comes a corresponding increase in the potential havoc wrought by denial of service, spam and other forms of cyberattack on the wireless infrastructure itself.

This paper explores some of the technical and operational challenges facing mobile operators (MOs) as they prepare their core network infrastructure for the provision of first 4.5G and then full 5G mobile services, with special focus on the security layers that necessarily underpin them.

PHASED MIGRATION VIA 4.5G

For most if not all operators, 4.5G is an essential step on the path to 5G. Requiring only minimal new hardware implementation, it offers a cost-effective way for MOs to meet some of the demand for higher capacity, while at the same time gaining familiarity with much of the new technology, architecture and operational changes required for 5G.

Of these changes, some, such as Massive MIMO and the utilization of unlicensed spectrum currently reserved for WiFi, all support the necessary adoption of higher frequency radio transmission.

Others concern changes to the mobile core, the overall architecture, its management and orchestration, and it is on these that this paper will now focus.

For this architectural migration, the existing 4G infrastructure of radio access and core networks, referred to respectively as LTE (Long Term Evolution) and EPC (Evolved Packet Core) will eventually be replaced by 5G NR (New Radio) and NGC (Next Generation Core). To achieve this there are several possible deployment options differentiated by the level of interworking supported between new 5G and existing 4G technologies. These can be broadly simplified into Standalone scenarios (SA), where only one radio technology is supported, and Non-Standalone (NSA), in which more than one is supported.

However, since the deployment of 5G cells and the corresponding adoption of 5G devices is unlikely to occur overnight, the NSA scenarios have the advantage of reducing time to market while ensuring optimal coverage and mobility.

COMMON TO ALL MIGRATION SCENARIOS WILL BE THE FOLLOWING TECHNOLOGICAL TRENDS:

- **The upscaling to Carrier-Grade Network Address Translation (CG-NAT) services** - required to compensate for the exhaustion of IPv4 addresses in the face of an IoT-driven explosion in the number of connected devices, as well as to provide additional security by cloaking the internal IP addresses.
- **Mobile Edge Computing (MEC)** – in which critical compute and storage resources are brought closer to the user to minimise latency and enable enhanced location-specific services and use cases such as autonomous transportation.
- **Cloud-RAN** – the virtualization of Radio Access Network functions.
- **Network Slicing** – the creation and customization of virtual networks to meet the many varied requirements of applications, services, devices and verticals.

SECURITY IMPLICATIONS OF THE MIGRATION

As the core network is transformed to support 4.5G and then 5G, we move from a predominantly physical infrastructure to a partially virtualized, hybrid infrastructure, and finally to a predominantly virtualized network. This has five main implications for the deployment of security functions:

Security VNFs

The security of agile new services delivered through dynamic software-defined virtual networks, requires the virtualisation of network security functions as well as their integration with domain and multi-domain management & network orchestration (MANO).

SDN Integration

Unlocking the full potential of Software Defined Networking (SDN), requires multi-vendor network components, implemented as either Physical Network Functions (PNFs) or Virtual Network Function (VNF), to integrate with a software-based, centralized control plane. Consequently, all security PNFs and VNFs must incorporate APIs or pre-integration to SDN ecosystems to provide security automation with consistent management and DevOps support.

ETSI NFV Architecture Integration

Due to the complexity and heterogeneity of next generation mobile infrastructure and services and the central use of ETSI's Network Function Virtualization (NFV) as its underlying management and orchestration framework, close alignment and integration with NFV components is essential.

Massive Security VNF Scaling

By decoupling the underlying hardware from its function, virtualization adds agility and flexibility, but can also reduce performance, predictability and availability. To overcome this requires the security VNFs' ability to dynamic scale in or out based on service requirements and load. And with the rapidly evolving, dynamic demands of future 5G services, this will need to happen on a massive scale.

Core Protocols Evolution

5G introduces a fundamental change in core signaling with the move from a point-to-point, monolithic signaling protocols architecture to a Service Bus Architecture (BSA) that facilitates agility and flexibility in network functions and services deployment and availability. 5G's uniform protocol stack is based on Internet stack with the replacement of core signaling protocols such as SCTP by TCP or Diameter by HTTP/2. The underlying security infrastructure must be able to support both existing 4G protocols and 5G protocols.

SECURITY IMPLICATIONS OF THE MIGRATION (Continued)

More generally, as the architecture changes, so too will the logical boundaries (also referred to as network reference points NG1 – NG16) at which carrier-grade firewall security must be applied. As with existing 4G mobile infrastructures, the security functions required to protect 4.5G and 5G mobile services will broadly fall into two main groups:

1

PROTECT AND PROVIDE INTEGRITY FOR CONTROL-PLANE COMMUNICATIONS.

2

PROTECT, INSPECT, AND PROVIDE INTEGRITY FOR DATA-PLANE COMMUNICATIONS (USER TRAFFIC) TO AND FROM EXTERNAL AND INTERNAL PUBLIC DATA NETWORKS (PDNS).

One of the most significant changes for these firewalls in the migration from 4G to 5G, will be the increase in sheer traffic volume – particularly across the NG6 interface to the Public Data Network (PDN).

In addition to mitigating the vulnerabilities and attack vectors listed below, these two functional units will need an ability to adapt to change faster than ever before. As the range of new 5G services explodes, the number of malicious threats and the level of resource and investment behind them, will likely show a parallel trend. Consequently, an automated ability to adapt to this evolving threat landscape will be essential to any future-proof security architecture.

VULNERABILITIES SPECIFIC TO THE EVOLVING MOBILE NETWORKS

As well as the usual vulnerabilities common to all IP networks, mobile service provision introduces specific additional risks:

Open Connection to 3rd-Party Roaming Partners

The growing adoption of massive scale technologies such as IoT, coupled with regulatory and competitive drivers such as the European “Roam Like at Home” directive, all drive the need for secure, massively scalable connectivity and interoperability with mobile roaming partners.

Greater risk from botnets

With the number and variety of connected devices set to explode, the ability of operators to test and vet them all will be challenged to the extreme. Consequently, malicious actors will be looking for exploits, which if found could unleash botnets of an unprecedented size and destructive potential.

Unsecured paths from unknown mobile devices

In the ‘flat’, IP-based architectures of LTE and 5G, the encryption from the User Equipment (UE) stops at the eNodeB (eNB) and gNodeB (gNB), leaving a clear IP traffic path all the way to the core. Coupled with the expected proliferation of countless different kinds of mobile/IoT devices, the associated risk will multiply exponentially.

TARGETED ATTACK VECTORS

GPRS Tunnelling Protocol (GTP)

As the principal means of carrying GPRS packets across the IP core network, GTP is an obvious vector of attack. Through malformed GTP packets, out of state GTP messages or simple IP spoofing, cybercriminals can launch denial of service or over-billing attacks and open the door to host of other threats. With the security of both control and data plane traffic at stake, GTP protection is an essential capability for both SeGWs and GiFWs.

Diameter

Diameter is the primary means of authentication, authorization and accounting (AAA) across the 4G mobile infrastructure. As such, any attack inhibiting its proper function (malformed messages, overload, creation of signaling storms etc.) can have serious consequences for mobile security including:

- Manipulation of service accounting and billing
- Denial of Service (DoS)
- Unauthorized connection to restricted core resources

Session Initiation Protocol (SIP)

As a key signaling protocol within the IP Multimedia Subsystem (IMS), SIP-based attacks have been increasing steadily over recent years. Although some of this increase represents opportunistic scanning for default or weak passwords on VoIP servers or end-points, SIP's clear-text message format makes it vulnerable to a range of other attacks including registration / session hijacking, server impersonation and message tampering. Such attacks can then be used to eavesdrop, deny service, defraud operators and more.

Stream Control Transmission Protocol (SCTP)

As the main transmission protocol used across multiple EPC and 5G-NGC signaling interfaces, as well as between roaming partners, SCTP is vulnerable to a range of threats including address camping, association hijacking and bombing attacks.

Domain Name System (DNS)

Due to their critical and central role in mobile core infrastructure for both control and data plane operations, attacks such as DNS floods can easily bring down the entire network. Also, just recently, LTE network vulnerabilities were discovered that could alter DNS traffic and reveal users' identities and web histories.

Internet Stack Protocols

According to an enisa report from March 2018 (Signaling Security in Telecom SS7/Diameter/5G), the use of common "Internet" protocols like HTTP, TLS and REST APIs will create a situation where "the grace period between vulnerability discovery and real exploitation will become much shorter compared to SS7 and Diameter". It is clear that 5G deployments will be more exposed to exploits and vulnerabilities brought by the use of open, Internet-based protocols.

SECURING 4G, 5G AND BEYOND - FORTINET SOLUTIONS OVERVIEW

Fortinet offers strategic security solutions specifically designed to address the unique challenges facing operators as they migrate their core networks to deliver 4.5G and 5G mobile services.

THROUGH A HIGH-PERFORMANCE RANGE OF BOTH PHYSICAL AND VIRTUAL NETWORK FUNCTIONS (PNF/VNF), FORTINET DELIVERS:

- End-to-end carrier-grade security designed for the massive scale of 5G mobile operator networks from the endpoint, through the mobile core, and to the cloud.
- Physical-to-hybrid-to-virtual network migration consistency facilitated by complete functional parity between the hardware-accelerated physical appliances and their VNF equivalents.
- Intelligence to actively secure service provider domains with a purpose-built operating system.
- Rich set of security capabilities for CSP-only protocols.
- Up-to-the-minute security intelligence via FortiGuard Labs to ensure protection against the ever-evolving cyber threat landscape facing mobile carriers and their customers.
- Simplified management, visibility, and analysis of mobile carrier networks and current threat profiles for both physical and virtual environments with FortiManager and FortiAnalyzer.
- SDN integration via Fortinet Connectors and Fortinet's APIs, which are available via the Fortinet Developer Network and include integration with Nuage Networks, Cisco ACI and VMware NSX.
- ETSI's MANO integration with major vendors such as Amdocs, Ciena/Blue Planet, HPE, Ericsson, Nokia and Cisco.

COMPLETE CONTENT AND NETWORK PROTECTION: FORTIGATE AND FORTIOS

A FortiGate NGFW implemented as either a PNF or a VNF is based on FortiOS security operating system which has all the features required to deliver next generation security plus the specific support for CSP-specific protocols.

TO FULLY PROTECT BOTH DATA AND CONTROL PLANES BETWEEN RAN/NR TO EPC/NGC AND WITHIN EPC AND NGC DEPLOYMENTS, FORTIOS INCLUDE SUPPORT FOR THE MAIN CAPABILITIES:

- GTP Firewalling
- Diameter Verification
- Security Gateway (SeGW)
- Gi-LAN NGFW & User Services
- Carrier-Grade SIP Security
- CG-NAT and IPv6 migration
- Next Generation security for “Internet-stack” protocols
- NGFW-based PNF/VNF for customer facing services
- IOT-specific Security
- Multitenancy with Virtual Domains (VDOMs)
- SDN and MANO integration
- Massive auto scaling PNF/VNF
- Lowest footprint and fastest boot time consolidated VNF
- HW-accelerated PNF

INTEGRATION WITH SDN, VNF MANAGEMENT AND NETWORK ORCHESTRATION (MANO)

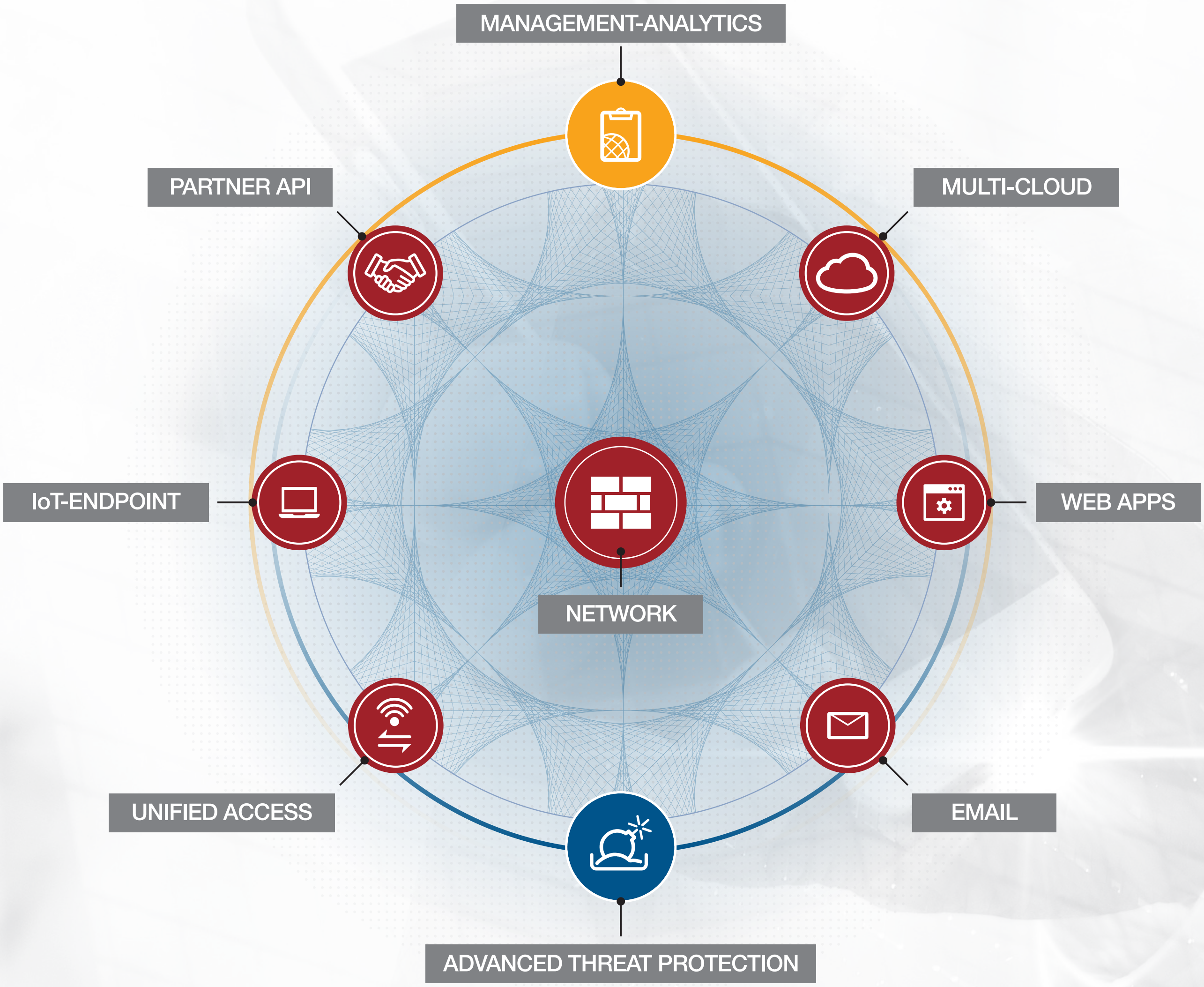
All Fortinet VNFs have demonstrated deep integration within life cycle operations - allowing Communication Service Providers to confidently deliver security as a service to their customers and within their network. Fortinet’s VNF span all major NFVIs, major MANOs, major SDN, and major public cloud providers.

Through Fortinet Technology Partners and Fabric Ready programs, CSPs have a wide choice of SDN and MANO security VNFs pre-integration with vendors such as Amdocs, VMware, Nuage Networks, Cisco, Ciena, Ericsson, Nokia, Cloudify, Rift.io and more.

This flexible and rich ecosystem of integrated partners reduces cost and time-to-market to deliver dynamic, on-demand and zero-touch security services.

STATE OF THE ART SECURITY WITH FORTINET'S SECURITY FABRIC

The rich feature set and capabilities delivered by FortiGate and FortiOS are complimented by Fortinet's Security Fabric, which integrated additional PNFs/VNFs with the broadness and automation required by 5G. These provide a complete ecosystem that adds additional security internal and external facing services and capabilities, such as Advance Threat Protection (ATP), Web Applications Security, strong authentication, etc.

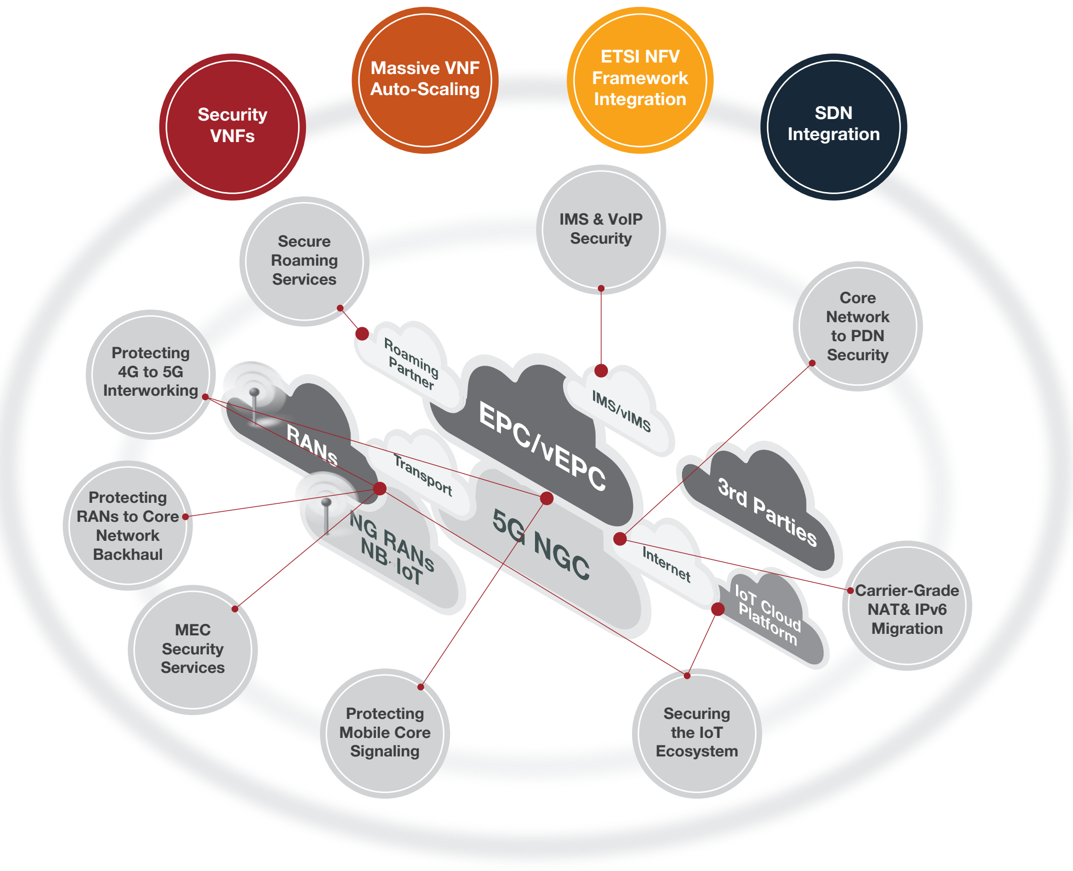


SUMMARY

The widespread deployment of 5G mobile services will be nothing short of revolutionary and the opportunities for those able to capitalize on this revolution are virtually boundless.

As CSPs are evolving and migrating their mobile infrastructure from 4G to 5G and beyond, the ever-present and evolving threat of cyberattack will require an underlying security infrastructure that can secure that migration with unprecedented levels of performance, scalability, agility, protection and cost effectiveness.

Fortinet security appliances are already securing 3G and 4G core networks on 5 continents. Established presence in this key market proves that Fortinet has not only the solutions for today but also has the technological, architectural and operational experience to support your 5G strategy.


Security VNFs
Massive VNF Auto-Scaling
ETSI NFV Framework Integration
SDN Integration
Secure Roaming Services
IMS & VoIP Security
Core Network to PDN Security
Protecting 4G to 5G Interworking
Roaming Partner
IMS/vIMS
EPC/vEPC
RANs
Transport
3rd Parties
Protecting RANs to Core Network Backhaul
NG RANs NB- IoT
5G NGC
Internet
IoT Cloud Platform
Carrier-Grade NAT& IPv6 Migration
MEC Security Services
Protecting Mobile Core Signaling
Securing the IoT Ecosystem

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard
#12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990