



5G Security, Openness and Trust Considerations

How an open and transparent 5G core design can bolster confidence

Published by

MOBILE
WORLD LIVE


Hewlett Packard
Enterprise

Executive Summary

Based on interviews with experts from Hewlett Packard Enterprise (HPE) and the GSMA, this paper discusses the design of 5G networks, the trust relationships between operators and vendors, and how to maximise security through technology, work processes and partnerships.

Realising the full benefits of 5G depends upon a dedicated core network, which is required to support advanced functionality, such as end-to-end manageability, the accommodation of multiple network technologies and network slicing. As the core controls who can access which services, it is the most sensitive part of the 5G network.

The effective brains of the network, the core is a potential treasure trove for espionage and a key target for sabotage attacks. Historically, it has been highly centralised and monolithic: Taking down only individual elements of the core could take down the full network. However, the advent of 5G offers operators the opportunity to move away from this model and employ a potentially much more secure and robust architecture.



In developing its new cloud-native 5G Core Stack, HPE has adopted the following principles:

Openness and transparency:

By utilising open standards and modular software functions, telcos gain increased visibility into their 5G system and can constantly adapt the most effective cloud-native security software to combat the dynamic evolving threat of hackers and bad actors. Given the continuous threat of attack, the important thing is that operators can see what is happening in their core network and react quickly. To that end, telcos need their core networks to be as transparent as possible. As they cannot assume trust in their vendors, operators need to maintain full visibility and full control of any changes. In particular, network functions need to be fully transparent. The cloud-native design used in 5G networks is a key enabler for this transparency.

Move away from monolithic black boxes: As 5G breaks up the traditional monolithic core into smaller micro-services

communicating over open interfaces, it is much easier for the operator to observe what is going on and audit transactions. Moreover, the containerisation of micro-services allows for finer grained monitoring of network functions to quickly identify any attempt to leak data or divert performance.

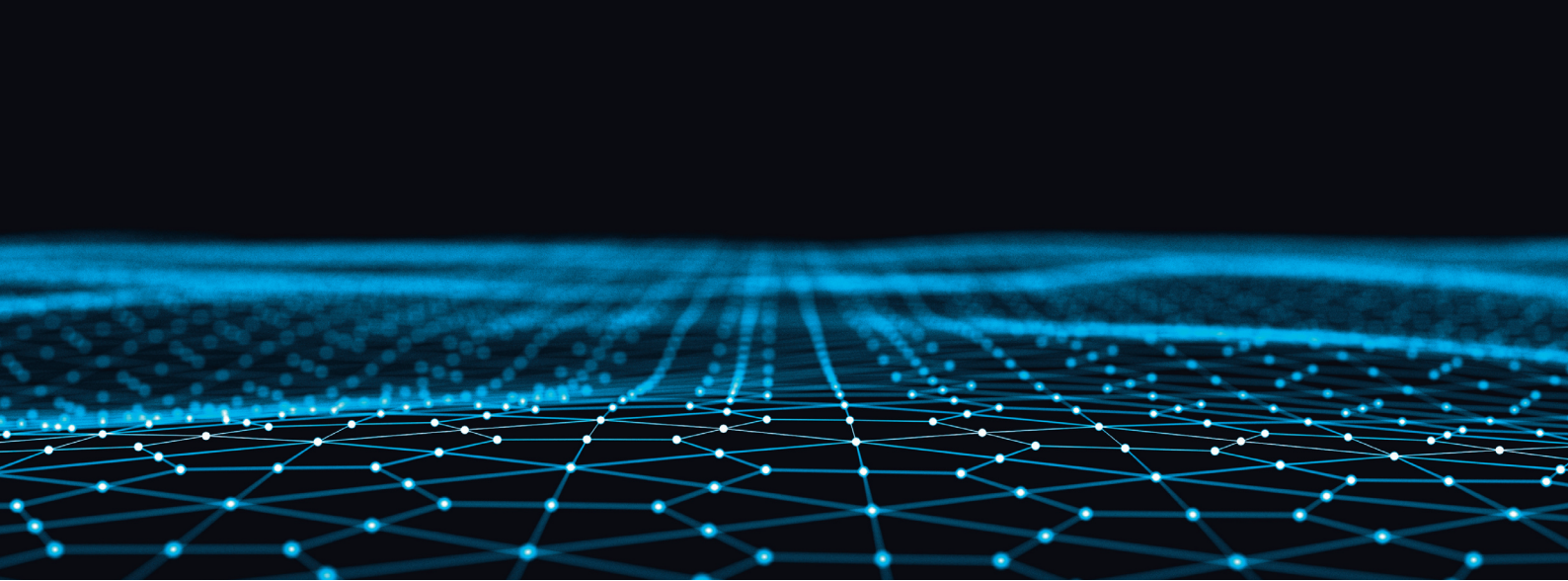
Managing continuous change:

No network is ever frozen: There is always a need to add more modules, upgrade software or install a patch. As any of these actions can be vehicles for inserting malware, operators need to have tools for continuous integrity-checks.

Multi-vendor – no lock-in: If an operator loses trust in a specific function in the network, and/or the associated vendor, an open architecture means it can swap-out and replace with a similar network function that it trusts. The architecture of 5G networks supports a shift to supply chain flexibility and a release from vendor lock-in.

Common security control: The separation of network function data from processing, together with its storage in a “shared data environment” makes the data easier to monitor, secure and control. This is very important for the key network functions involved in network access and authentication. By controlling these centrally, as part of the shared data, they are harder to hack.

Silicon root of trust: Critical functions can be further protected using a mechanism called “silicon root of trust.” Embedded cryptographic firmware can be designed to mitigate any attempt to run foreign software or hack into the function. The idea is that each server checks itself while it starts, to verify that the start-up process contained in its chips matches the known good configuration from the factory. In this way, silicon root of trust limits potential supply chain vulnerabilities and hacking attempts.



1. The Rollout of 5G

Mobile operators across the world are deploying 5G networks. This highly versatile and capable connectivity can deliver entirely new digital experiences in cities, venues, healthcare facilities, campuses, at work, and in the home. As well as transforming the lives of individuals, 5G promises to deliver substantial improvements in functionality and operational efficiency across industry. For example, smart factories are increasingly using connected equipment and supply chains to produce goods more quickly, safely, and inexpensively, while augmented reality services can overlay virtual content on top of real-world objects to enable new kinds of training, education, working, and gaming.

Such services will become increasingly viable as 5G creates smarter networks that understand and adapt to the services running on them. With 5G, networks can reorganise and reconfigure themselves in seconds, to deliver the right resources to the right place at the right time.

But the likely pervasiveness of 5G will bring risks. With connectivity everywhere, bad actors will try and take control of 5G networks to steal data and mount cyber-attacks on individuals, organizations and governments.

What makes 5G different?

While previous generations of cellular networks relied on proprietary, integrated systems from a small number of incumbent suppliers, 5G standards are designed to take advantage of open, cloud-native platforms that allow mobile operators to deploy new 5G services faster and in a more flexible way. 5G is:

Open by design: With earlier generations of mobile networks (2G, 3G and 4G), some operators found themselves locked into their equipment vendors' closed, proprietary ecosystems. Once a vendor had been selected, it could be hard to integrate its products and solutions with those of other vendors, increasing costs and, potentially, stifling innovation. By contrast, 5G is designed to be "open" and software-driven, letting operators mix and match technology from any vendor. Indeed, 5G networks can utilise commercial off-the-shelf servers along with modular software components from different vendors, potentially enabling telcos to monetise new 5G services faster.

Heavily dependent on cloud

technologies: Some of the most innovative capabilities of 5G networks, such as the ability to provide customers with dedicated slices of connectivity, stem directly from running telecom networks as

a malleable cloud-based service, similar to the way in which major technology companies, such as Google and Facebook, run their services. Cloud-native networks can use flexible IT technologies, such as micro-services and containers, which combine an application with all of its related configuration files, libraries and dependencies to enable it to run in an efficient and reliable way across different computing environments. In effect, the telecoms sector can draw on best practice from the IT sector, where cloud-native and open source solutions have been widely adopted.

Smarter and more flexible:

Whereas earlier generation networks were basically "one size fits all," 5G can deliver all kinds of "virtual" networks, each tuned for a specific kind of service, over the same infrastructure. Operators can segment their networks, as if they were lanes on a motorway, designating some for the fastest, most critical traffic, such as communications with vehicles or drones, while optimising others to provide low cost connectivity for more tolerant, less time-sensitive use cases. With this flexibility, operators and enterprises can collaborate to create new, customised business services that couldn't exist before.

2. Industry view on 5G security

Experts say one of the distinctive features of 5G is its holistic approach to security – the standard has been designed to anticipate the security challenges of the future, as well as building on the security enhancements realised in each of the earlier generations. Jon France, head of industry security at the GSMA, describes 5G as bringing about a step change in security. “When we move to standalone 5G, that is the revolutionary piece,” he explains.

A lot of thought on security has gone into the design of 5G, with stronger encryption, mutual authentication between the network and the edge device, integrity protection and a service-based architecture for the network.

In fact, 5G employs security mechanisms and protocols used in state-of-the-art IT systems. “It is definitely borrowing a lot of security concepts from the IT world, while allowing that world to benefit from inherently secure telecoms connectivity,” says Jon France.

Such precautions are critical because the threat landscape will be much broader with 5G, partly due to the richness of the services and the much greater number of devices that will connect to 5G networks, many of which will be IoT, and the volume of traffic that will be generated. “That means there is an increase in the challenge in spotting rogue and errant traffic in the greater data volumes,” Jon France adds. “There is complexity with the breadth of services with 5G, and the speed they will operate at, in that data can be downloaded far faster with 5G, so you have a smaller window of opportunity for detection.”

As the world becomes increasingly reliant on connectivity, another key challenge is “poor mainstream digital literacy” according to security experts canvassed by GSMA Intelligence, the research arm of the GSMA. “There are concerns about the talent pool – whether you have got the skills out there to secure the networks,” explains Mark Little, a senior manager with GSMA Intelligence. “There is a new generation of toys that engineers need to learn how to play with.”

Although he notes that security is now much higher on the industry’s agenda and there is a greater focus on security-by-design, Mark Little is concerned that in the competitive race to deploy 5G networks we could see security lag behind in deployments. “The bad guys love it whenever there is a new field of battle,” he adds. “There will be new attack vectors that experts won’t have even thought about, so there has to be an expectation that the black hats will find holes. But the strategic move to open and transparent networks, and the security innovations that potentially enables, should put the good guys in a position to fight back.”

At the same time, some governments have major concerns about the provenance and ownership of the telco equipment providers supplying domestic network infrastructure. They worry that 5G network equipment will be used to leak information to foreign entities, or attack the network from within.

The importance of securing the 5G core network: In the initial rollout of 5G, the industry has focused on the new radio technology, but realising the full benefits of 5G also depends upon a dedicated core network, which is required to support advanced functionality, such as end-to-end manageability, the accommodation of multiple network technologies (4G-5G coexistence) and network slicing.


As the core controls who can access which services, it is the most sensitive part of the 5G network. The core is essentially the brains of the network, controlling subscriber access, collecting usage information and setting usage policies. That makes it a potential treasure trove for espionage.

By contrast, the radio access network, transport and edge elements of the network are geographically distributed by definition. The radio access network uses encryption by design, while risks can be further mitigated by segmenting the network and using multiple suppliers.

Historically, the core network has been highly centralized and monolithic: Taking down individual elements of the core could take down the full network (see diagram on page 6). But 5G allows for network slicing, meaning different sources of traffic can be kept separate, both logically and physically when using virtualisation and containerisation, thereby providing a first level of mitigation against attack.



A lot of thought on security has gone into the design of 5G, with stronger encryption, mutual authentication between the network and the edge device, integrity protection and a service-based architecture for the network.



	Sabotage	Espionage	% of total network cost
RAN & Transport	Partial outage	Limited	~80-90%
Edge Cloud	Partial outage	Limited	<10%
Core Network	Full outage	Full access	<10%

3. How to secure the 5G Core

Key principles

Experts at HPE point to several principles that will help to design security into a 5G core network:

Openness: It may seem counterintuitive, but the openness of 5G networks could make them more secure. By utilising open standards and modular software functions, telcos gain increased visibility into their 5G system and can constantly adapt the most effective cloud-native security software to combat the dynamic evolving threat of hackers and bad actors. Given the continuous threat of attack, the important thing is that operators can see what is happening in their core network and react quickly. “As operators can’t outsource this responsibility to their network vendors, they need to have tools and architecture that let them monitor, verify, mitigate, and act on threats,” says Mark Syrett, the security officer and 5G security architect for Communication and Media Solutions at HPE. “With open networking, risks can be monitored, mitigated and addressed at all levels: The elements of the networks; the work processes around them and the vendors involved.” For example, in the case

of work processes, openness enables operators to rigorously monitor any change to software or hardware before it is introduced into the live network.

Transparency: Telcos need their core networks to be as transparent as possible. As they cannot assume trust in their vendors, operators need to maintain full visibility and full control of any changes. In particular, network functions need to be fully transparent. The cloud-native design used in 5G networks can enable this transparency.

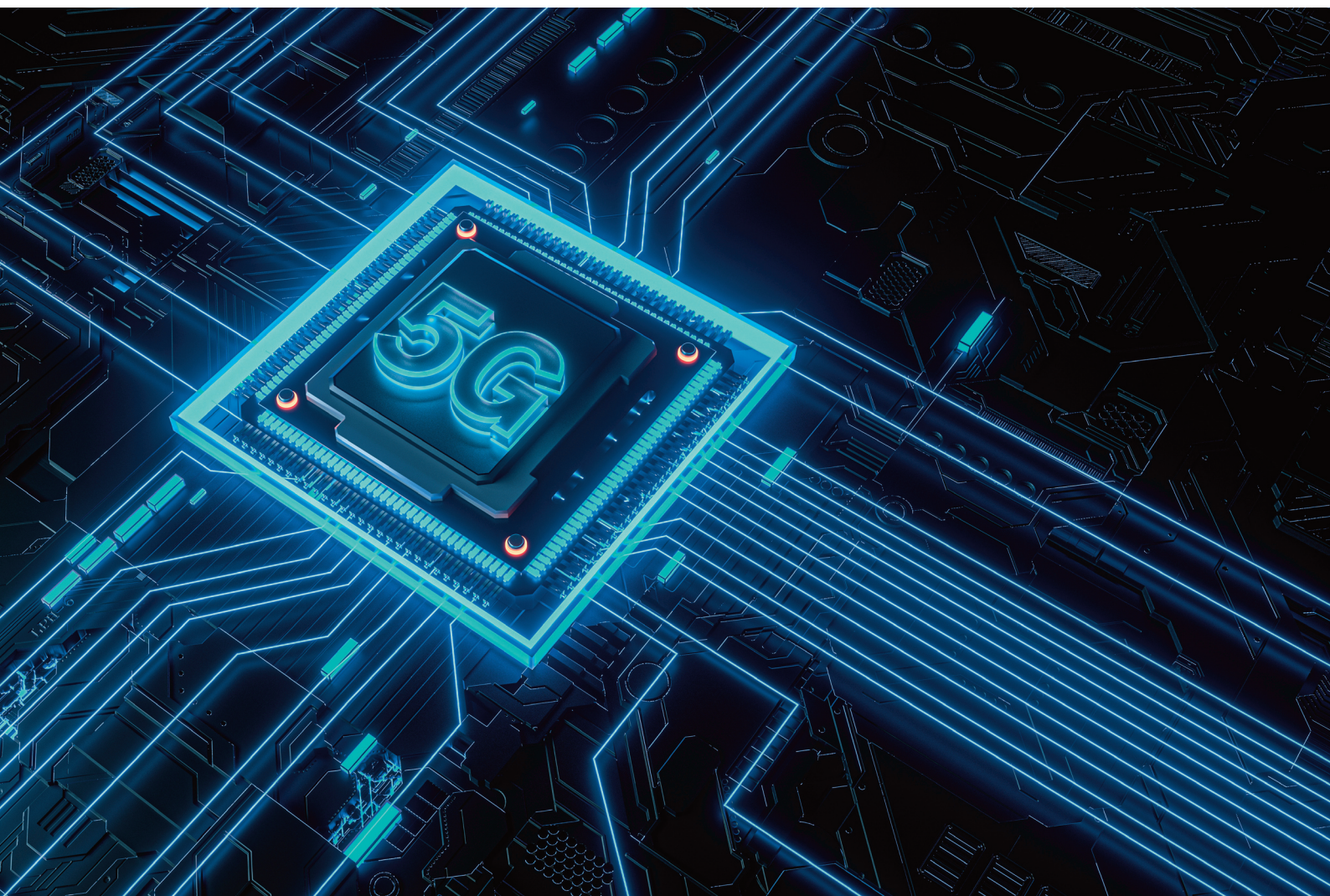
Move away from monolithic black boxes: Traditionally, the core of a mobile network has been composed of a small number of large network functions each with their own security provision. But 5G breaks up this traditional monolithic core into smaller micro-services communicating over open interfaces, which makes it much easier for the operator to observe what is going on and audit transactions. Moreover, the containerisation of micro-services allows for finer grained monitoring of network functions to quickly identify any attempt to leak data or divert performance.

Managing continuous change: No network is ever frozen: There is always a need to add more modules, upgrade software or

install a patch. As any of these actions can be vehicles for inserting malware, operators need to have tools for continuous integrity-checks. Continuous integration (CI) and continuous delivery (CD) frameworks, together with the integration of software development and IT operations (known as DevOps), can be used to support such checks.

The continuous deployment of small changes can help to control risks and patch vulnerabilities
notes Mark Syrett

Multi-vendor – no lock-in: If an operator loses trust in a specific function in the network, and/or the associated vendor, an open architecture means it can swap-out and replace that function with a similar network function that it trusts. The architecture of 5G networks supports a shift to supply chain flexibility and a release from vendor lock-in.



Further safeguards

Common management of security functions: The separation of network function data from processing, together with storage in a “shared data environment” makes the data easier to monitor and secure. The same applies to key security services, such as authentication and auditing, and network functions, such as the Authentication Server Function (AUSF), the Unified Data Manager (UDM) and Unified Data Repository (UDR). If these functions are controlled centrally, as part of “shared data environment”, they should be harder to hack.

“The core network is pretty fundamental – a lot of the protections are enabled in the core,” notes Jon France of the GSMA. The move to an open architecture “means it absolutely can be more secure. The building blocks of the core, network functions, are designed to integrate with each other with security in mind. Also due to Extensible Authentication Protocol (EAP) non-telco network components can interface with security protections...you have a crossover between IT and telecoms in which the two can be integrated. For example, there can be seamless security between a Wi-Fi connection and a 5G connection.”

4. The Hewlett Packard Enterprise 5G Vision

HPE's 5G vision is based on four fundamental principles: open, secure, proven, and delivered as-a-service. HPE provides hardware and software that is decoupled from proprietary systems to help telcos transform their legacy networks into a service-based architecture ready for 5G.

HPE offers a broad portfolio of solutions spanning the telco core, the telco edge and into the enterprise. Built on open and interoperable platforms combined with carrier grade infrastructure and modular software components, HPE's portfolio is designed to enable customers to incorporate more automation, reduce operational costs, become more agile, and deploy new 5G services faster from edge to core, while

virtualising the radio access network RAN and extending 5G connectivity into the enterprise with Wi-Fi 6.

HPE says its 5G architecture is open by design, which means that all traffic and performance patterns can be monitored for information leakages or unauthorised activities, with no "black-boxes" to hide malware.

HPE's 5G-Core solution

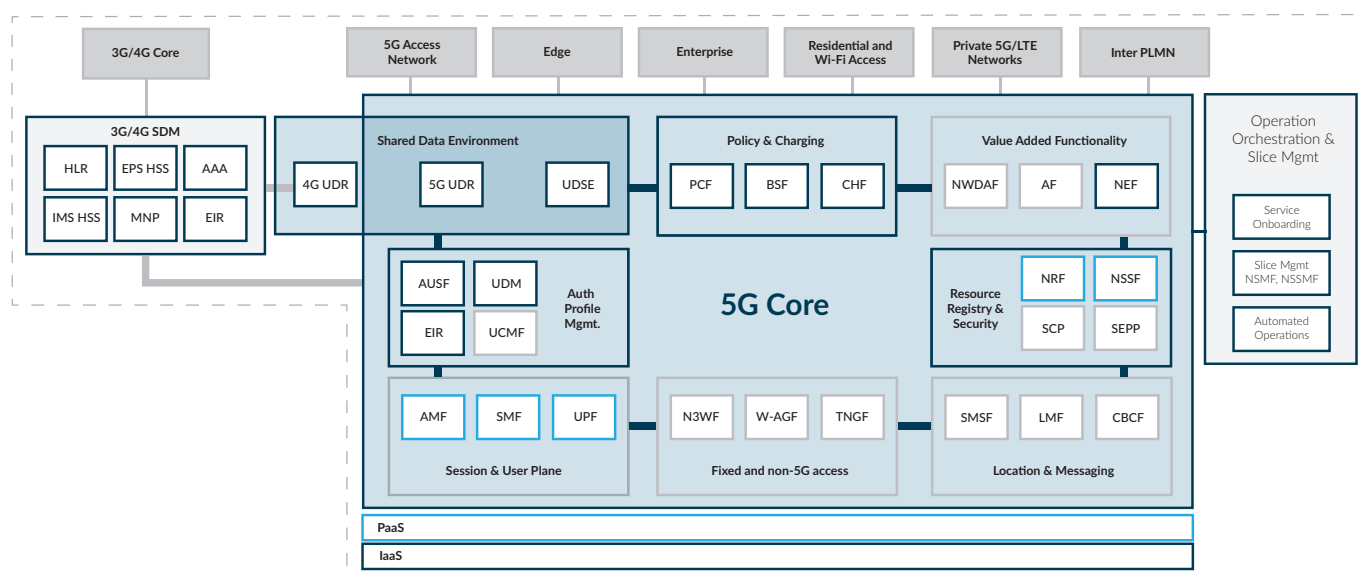
HPE says its complete 5G-Core (see diagram on page 9) has three very important characteristics:

1. Cloud-native from the ground up, which allows total openness and scalability
2. Multi-vendor and modular by design: so customers are free to include network functions from any vendors, for best-of-breed functionality with no vendor lock-in.
3. Shared data environment, which acts as a central layer for information keeping and authentication functions.



HPE 5G Core - Reference Architecture

End-to-end functional schema



Launched in 2020, HPE 5G Core Stack is designed to be a full end-to-end 5G-core solution that follows the security principles outlined in the previous section of this paper. Its open design ensures full transparency, while all the network functions are implemented as micro-services that are logically containerised and constantly monitored. HPE has broken up the attack surface by integrating stateless network functions from multiple vendors on a common service based architecture and shared data environment.

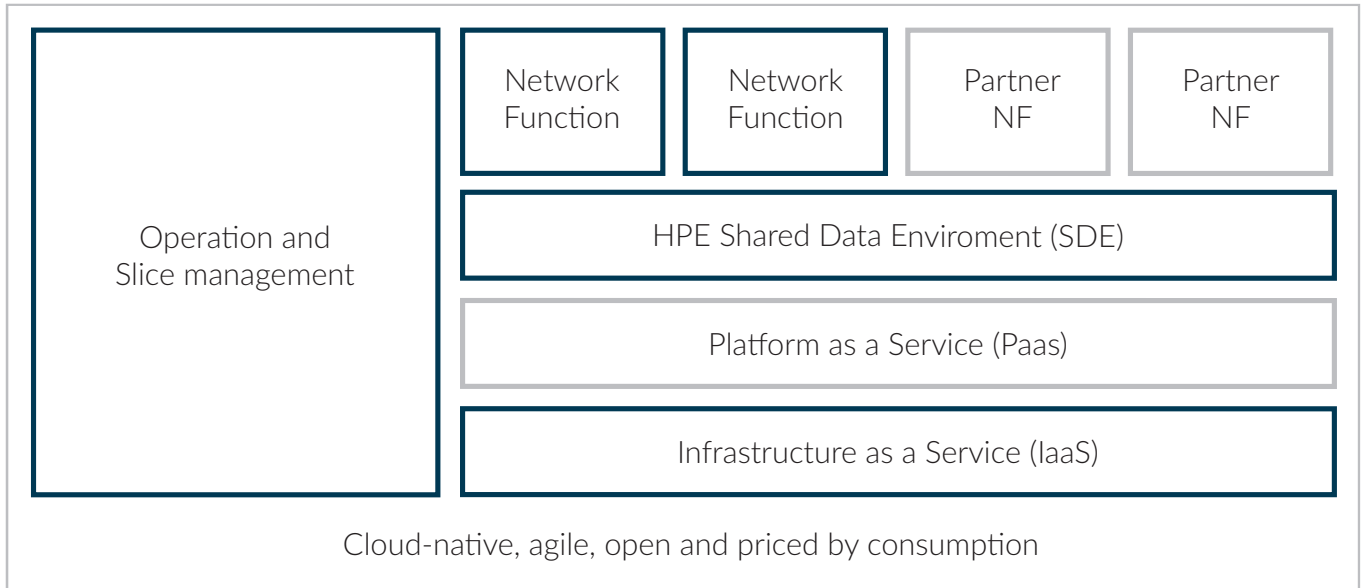
With no “black-boxes”, operators can inspect both the performance of the functions and the traffic going through them and identify any attempt to leak data, or divert from normal performance.

The HPE 5G architecture elements are built for continuous verifications, via DevOps and CI/CD methodologies, allowing operators to perform rigorous inspections processes using a variety of automation tools.

Pre-integrated with HPE and partner network functions, the container-based software stack is cloud-native from the ground up, with an open multi-vendor design. HPE says the pre-integration reduces the risks of security misconfiguration (for example, Kubernetes pod policy, API access control, clusters and helm charts) to make it secure by default.

HPE 5G Core Stack is designed to provide 5G operators with the core network capabilities, including end-to-end network slices, required to rapidly deliver new 5G services to subscribers and enterprise customers. HPE says it can be seamlessly integrated with previous generation networks and support upcoming advances in 5G standards.

HPE 5G Core Stack Solution Pre-integrated 5G Core



 HPE function  Partner function

The use of an open cloud-native model with stateless network functions is designed to enable operators of 5G networks to separate the data from the network functions and maintain it in a shared data environment. This affords interoperability with other networks (4G, Wi-Fi 6), and allows operators to integrate software updates on a much faster cycle.

HPE says its shared data environment is a key design element for managing shared subscriber profiles across the network.

“

Mark Syrett, explains:

One demonstration of HPE's leadership here is in 3GPP Release 16 where we led the specifications for another critical data component in this Shared Data Environment – the UDSF (Unstructured Data Storage Function) to allow even greater control over data.

”

The HPE 5G Core Stack is developed, integrated and delivered to customers via a continuous-integration and continuous-delivery (CI/CD) DevOps methodology. HPE says DevOps is a good fit with an open solution approach, as it helps developers, integrators and operators to maintain control over software from multiple sources, such as 5G core systems, integration partners, open-source platforms, third-party solutions that are in the network and operator-owned systems.

Furthermore, HPE supplies telco-grade servers that include a silicon root of trust built into the hardware. Designed to detect and prevent tampering, the silicon root of trust provides a series of trusted handshakes from the lowest level firmware.

HPE's approach has won praise from industry analysts. In April 2020, IDC wrote

“

HPE 5G Core Stack changes the way network infrastructure can be purchased and deployed.... the cloud-native, containerized microservices architecture that the HPE Core Stack brings means that an E2E (end-to-end) network function and operations management solution can be deployed by any organisation. If fully embraced, such a combination is destined to reshape the global communications SP (service provider) industry.

”

IDC, 5G Operational Readiness: HPE's Core-to-Edge Network Infrastructure and Operations Management Solution", doc # US46143620, March 2020

Conclusion

The open cloud-native architecture of 5G has given the telecoms industry a golden opportunity to combine security best practice from the IT world with long-standing safeguards from the telecoms sector, such as the encryption used by radio access networks. “The design principles make 5G more secure,” notes Jon France of the GSMA. “That means it has a definite leg-up straight out of the gate.”

But 5G operators can't take security for granted – as cellular connectivity plays an increasingly vital role in a nation's socio-economic activities, it will be an increasingly tempting target for bad actors. In light of that, it will be particularly important for operators to carefully monitor their 5G core networks and ensure they have full control over both the hardware and software they employ.



Produced by the mobile industry for the mobile industry, Mobile World Live is the leading multimedia resource that keeps mobile professionals on top of the news and issues shaping the market. It offers daily breaking news from around the globe. Exclusive video interviews with business leaders and event reports provide comprehensive insight into the latest developments and key issues. All enhanced by incisive analysis from our team of expert commentators. Our responsive website design ensures the best reading experience on any device so readers can keep up-to-date wherever they are.

We also publish five regular eNewsletters to keep the mobile industry up-to-speed: The Mobile World Live Daily, plus weekly newsletters on Mobile Apps, Asia, Mobile Devices and Mobile Money.

What's more, Mobile World Live produces webinars, the Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and exclusive home to all GSMA event keynote presentations.

Find out more at www.mobileworldlive.com



**Hewlett Packard
Enterprise**

HPE has over 30 years of experience in the telecoms industry, with more than 300 telco customers across 160 countries. In the core, more than 700 million subscribers across more than 80 carriers depend on HPE Mobile Core software. HPE's open telco solutions help operators evolve their networks and services to a 5G ready, cloud-native, service-based architecture. As the edge-to-cloud platform-as-a-service company, our experience in hybrid cloud allows us to bring the cloud transformation and secure, carrier-grade, standards-based infrastructure to telecommunications networks.

Hewlett Packard Enterprise is the global edge-to-cloud platform-as-a-service company that helps organizations accelerate outcomes by unlocking value from all of their data, everywhere. Built on decades of reimagining the future and innovating to advance the way people live and work, HPE delivers unique, open and intelligent technology solutions, with a consistent experience across all clouds and edges, to help customers develop new business models, engage in new ways, and increase operational performance.

Learn more at hpe.com/info/5G

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

© 2020