STRATEGY ANALYTICS
Celebrating 25 Years of Insights

Networks and Service Platforms

amdocs

Service Providers Leverage Network Functionality to Expand 5G Value Plane with NEF and NWDAF

03 September 2021

Report Snapshot

This White Paper describes how Communications Service Providers (CSPs) can leverage 5G Standalone (SA) network functionality not only for efficient, highly automated network operations, but also to expand new service revenue opportunities.

By building a 'Business Bridge' for monetization, CSPs can create significant service value to complement and compete with Hyperscale Cloud Providers (HCPs).

This report discusses how two specific 5G SA Network Functions - Network Exposure Function (NEF) and Network Data Analytics Function (NWDAF) can enhance four service categories to capture these opportunities.

Contents

Executive Summary

Communications Service Providers (CSPs) are seeking ways to stimulate revenue growth with new 5G services as they simultaneously establish partnerships with the Hyperscaler Cloud Providers (HCPs) – AWS, Google Cloud, MS Azure etc. to reach new Enterprise users.

However, CSPs sorely need to add unique value and high value service enablers that will keep them part of the HCPs applications and enterprise services value chain to avoid becoming 'bit pipes to the Cloud'. Fortunately leveraged by 5G Architecture, they are now able to address HCPs top three networking concerns - ***Network Security, Operational Monitoring and Troubleshooting*** and ***Application Delivery Services*** including ***Load Balancing etc.***

For the first time in the history of telecoms, 5G Standalone (SA) cloud native service platforms make it possible for CSPs to '*Platformize' internal CSP Network Functions (NFs) and provide secure trusted access to 3rd party Cloud Hosted or private Enterprise Apps***.** They are therefore able to offer access to internal network control plane functions and allow Enterprises and HCPs to safely *modify their own service feature combinations* via Network Exposure Function (NEF) or to *capture their own analytics data* via Network Data Analytics (NWDAF).

This report examines the opportunity for those two particular Network Functions (NFs) NEF and NWDAF to *deliver both significant operational capabilities* and at the same time *significantly help to create new 5G service value*.

The four categories of services reviewed in the report will be among the most significant 5G SA Revenue generators in the long run. They are ***Network Slicing, Cloud Enablers, Edge Services*** and ***User Configurable Services***. Each of the four critically depends on the network based capabilities enabled in part by NEF and NWDAF functionality and summarized below:

- ***Network Slicing*** depends on *inherent 5G Security and Privacy mechanisms* to avoid commoditization while achieving 20 – 30 percent savings from *Virtualization and Dynamic Resource Management*.
- ***Cloud Enablers*** depend on *Dynamic Compute* and *Storage Allocation* 'at the edge' and across the metro area to create a 'Telco Connectivity Cloud' that adds significant value to the Hyperscaler's 'Data Center Cloud'
- ***Edge Services*** rely on Carrier Class response times with single digit milliseconds (ms) for Control Plane and Service Event responses to assure performance for low latency Apps. and state aware instantaneous recovery – in contrast to Round Trip Times (RTT) of 200 ms and potential packet loss in the 'Best Effort' Public Cloud
- ***User Controlled Service Options and Policies*** will eventually evolve to allow user or CIO configuration of ***Service Function Chaining on Demand*** – a truly cloud native hyper scalable service.

While the example services described in this report may *not look like the traditional end user 'Killer Apps' that CSPs continuously seek and rarely find*, they are all likely to generate significant revenue as enablers for CSP managed Private Networking, Cloud and Edge services as well as 3rd Party Vertical industry solutions. These services are likely to be very 'sticky' as they become embedded in Enterprise and HCP solutions and grow in value as part of those *customers' own digital transformation*. CSPs can in turn expect these capabilities to translate to enhanced revenues and margins for themselves through 2026.

I. Introduction

As 5G Infrastructure continues to be deployed successfully, Communications Service Providers (CSPs) are increasingly concerned about the lack of revenue growth from 5G bandwidth alone. They are now focusing on ways to leverage 5G not only to lower CAPEX per GByte and to reduce the cost of operations through automation, but also seeking ways to stimulate revenue growth with new 5G services.

To avoid sub-scale Data Center operations, reduce deployment costs 'at the edge' and in the hope of gaining a Go to Market channel to Enterprise customers many CSPs have established partnerships with the Hyperscaler Cloud Providers (HCPs) – AWS, Google Cloud, MS Azure etc. Several CSPs are now even hosting their 5G Core service platforms at HCP Data Centers and looking to co-locate their RAN network components with Cloud 'Edge Services' platforms e.g. AWS LocalZone servers very close to enterprise end users.

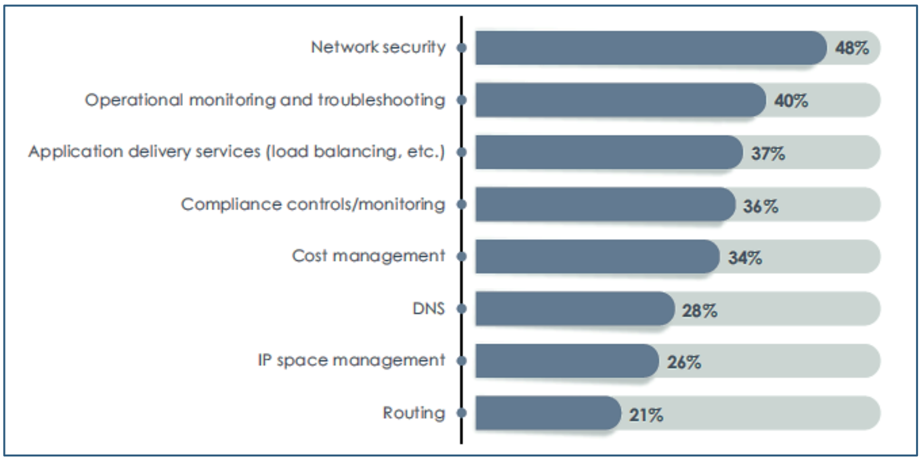
However, the HCPs have the strongest Enterprise relationships and host most Enterprise high value IT Applications. Many even provide Hybrid or Multi-Cloud access. This leaves CSPs on track to become '*commodity bit pipes to the Cloud*'.

CSPs therefore sorely need to add unique value and high value service enablers that will keep them part of the HCPs applications and enterprise services value chain.

Network based Priorities for Cloud Hyperscalers

Fortunately CSPs are now able to leverage 5G Architecture to address HCPs top three networking concerns as shown in the Chart below. The three concerns are ***Network Security, Operational Monitoring and Troubleshooting*** and ***Application Delivery Services*** including ***Load Balancing etc.***

Chart A. Aspects of cloud networking that most benefit from effective collaboration between network and cloud



Source: EMA Custom Research Report[7] *'A House Divided: Dysfunctional Relationships Between Network and Cloud Teams Put Cloud Strategies at Risk' Sponsored by Blue Cat Networks April 2021*

High value Control Plane Enablers keep CSPs in the Cloud Hyperscaler value chain.

As noted in a recent Webinar[1], HCPs success has been in large part due to their 'Platformizing of Cloud Tools' to make it easy for IT departments to migrate monolithic host computer software and applications 'to the Cloud' using generic capabilities such as containerization that avoid the need for labor intensive software rewrites.

For the first time in the history of telecoms, 5G Standalone (SA) cloud native service platforms make it possible for CSPs to '*Platformize' internal CSP Network Functions (NFs) and provide secure trusted access to 3rd party Cloud Hosted or private Enterprise Apps*. They are therefore able to leverage access to internal network control plane functions and allow Enterprises and HCPs to safely *modify their own service feature combinations* via Network Exposure Function (NEF) or to *capture their own analytics data* via Network Data Analytics (NWDAF).

As noted in an earlier Insight[2] "(CSPs) can now begin to leverage 5G management and orchestration to enable new services and assure their quality in minutes not weeks or months." Control Plane functionality and Analytics can now create monetizable customer value. And with 5G SA, authorized functions can be under customer control. IT Executives at Enterprises and HCP sites can soon control multiple network service and connectivity features or pro-actively monitor network Service Level Agreements (SLAs) just as they do today for the Cloud Data Center services – *as soon as they become trusted CSP partners.*

II. 5G Control Plane Builds 'Business Bridge' from Network to Value

As these 5G SA cloud native Network Functions (NFs) are deployed in late 2021, 2022 and beyond, CSPs will be able to trigger true *digital transformation for their customers' own value chains* as they capture for themselves new control plane based service value and revenue generating 'metadata' based applications.

This report examines the opportunity for two particular NFs to deliver both significant operational capabilities and at the same time create new 5G service value. The two functions are the Network Exposure Function (NEF) and the Network Data Analytics (NWDAF) functions.

5G Service Based Architecture creates new ways for CSPs to add Value

3GPP Release 16 ushers in a new phase for 5G services, further leveraging the 5G SA cloud native *Service Based Architecture (SBA)*. In an earlier report[3] Strategy Analytics described how each network function (NF) requests and delivers service capabilities to or from other functions via *Service Based Interfaces* (SBIs). The NFs each register their services with the *Network Repository Function* (NRF) and those services can then be discovered by other NFs. In conjunction with the NRF, the *Network Exposure Function* (NEF) plays a critical role to determine and orchestrate which NFs may interoperate with the outside world in order to perform higher-order API-driven procedures. NEF acts as the '*service gatekeeper'.*

In 5G SA, functionality is abstracted from any particular physical network node or dedicated point-to-point connection, and *any function can request services from any other authorized function*. A logical sequence of function requests and responses links together to form a *Service Function Chain (SFC)* and so creates an End-to-End (E2E) service. This 'flat architecture' allows every NF to provide its own capabilities to every other authorized NF and even – as we discuss below - to authorized external *Application Functions* (AFs) that are allowed to request the NF's services. This ***uniquely flexible but inherently secure architecture*** **allows CSPs to safely expose services and 5G capabilities both for internal use and for external authorized 3rd party Apps.**

Critical for CSPs to add network based value to Hyperscaler Cloud Services

As noted above, CSPs have begun to work more closely with the Hyperscaler Cloud Providers (HCPs) who are now hosting some of their 4G and 5G service platforms 'at the Cloud Edge' as well as in their regional Data Centers. 5G SA allows CSPs to offer *additional real time, state aware network-based differentiators to these HCP partners including* NEF and NWDAF. NEF was briefly described above.

NWDAF is a 5G Core NF that collects and provides access to past and present data from other NFs that are part of the 5G Core, specifically the NRF, the *Session Management Function* (SMF), *Access and Mobility Function* (AMF), *Unified Data Management* (UDM), *Policy Control Function* (PCF), *Application Function* (AF) as well as inputs from the traditional *Operation, Administration and Management* (OAM) system and the NEF. See Appendices A and B for additional details.

NWDAF information has many applications. For example NWDAF data may be used to monitor compliance of individual *Network Slice Instances* (NSIs) to guarantee Service-Level Agreement (SLA) quality and performance parameters. Operators often go a step further and use NWDAF information to both *proactively predict changes in slice performance parameters* and to *pre-emptively reallocate resources to avoid SLA violations*. The NWDAF itself can also present predictive inference outputs from embedded machine learning (ML) models that can be used subsequently to develop AI algorithms and optimize network performance. In addition to *Network Optimization*, NWDAF provides inputs for high value network applications to perform *Anomaly Detection* prior to a Physical Network Function (PNF) failure so as to avoid imminent network resource overload or potential outages.

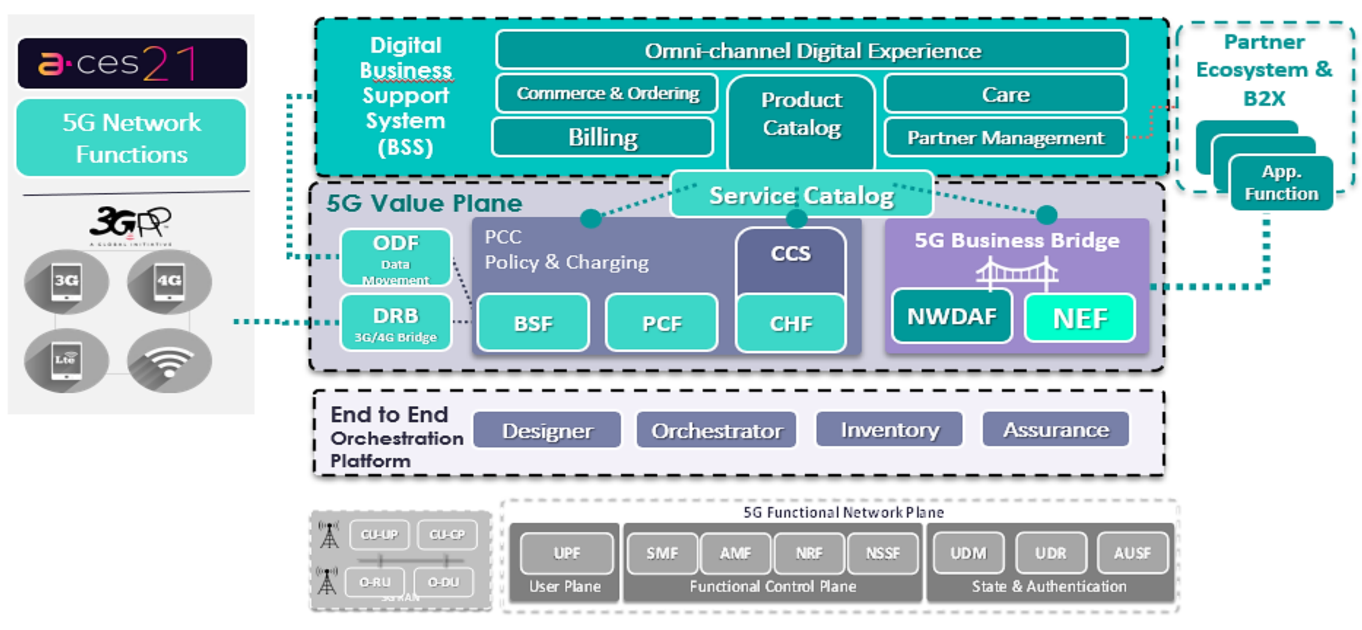
Now is the time for CSPs not only need to leverage both NEF and NWDAF themselves to ensure superior performance, but also to help their Enterprise and HCP customers leverage that network functionality to create their own value. To see how this can be achieved it is important to understand the joint role of NEF and NWDAF in forming the *Business Bridge* as part of the *5G Value Plane*.

5G Value Plane

In a special TMForum report in March 2021 report[4], Amdocs describes the *5G Value Plane* as "a key enabler for driving network-embedded services and bringing cloud business models to 5G networks. …5G SA core contains many functions that just power the network – or just make 5G work – (but that can also) tap into the wide revenue potential enabled by the new functionalities. (and as a) business consideration … become an integral part of the new core… driving the … 5G Value Plane."

The chart below shows the *Value Plane* in the middle sitting above the 5G *Functional Network Plane* with the standard 5G SA *User* and *Control Plane Functionality* below. The Value Plane includes the critical policy and charging functions as well as the critical *5G Business Bridge* role of *NEF* and *NWDAF* as they interface to the *Application Functions* (AFs) and via the *Service Catalog* to the *Business Support System* (BSS).

Chart B. 5G Value Plane connects the 5G *Functional Network Plane* (at the bottom of the chart) with *Service and Product Catalogs* and the *Application Functions* (AFs) for Partners and Developers on the upper right. In addition, *Policy and Charging, NWDAF* and *NEF* constitute the '*Business Bridge'* in the Value Plane.



Source Openet Division of AMDOCS

The 5G '*Business Bridge'* provides the critical point where new *Application Functions* (AFs) can be authorized for access to session and resource management by the NEF and for analytics by NWDAF.

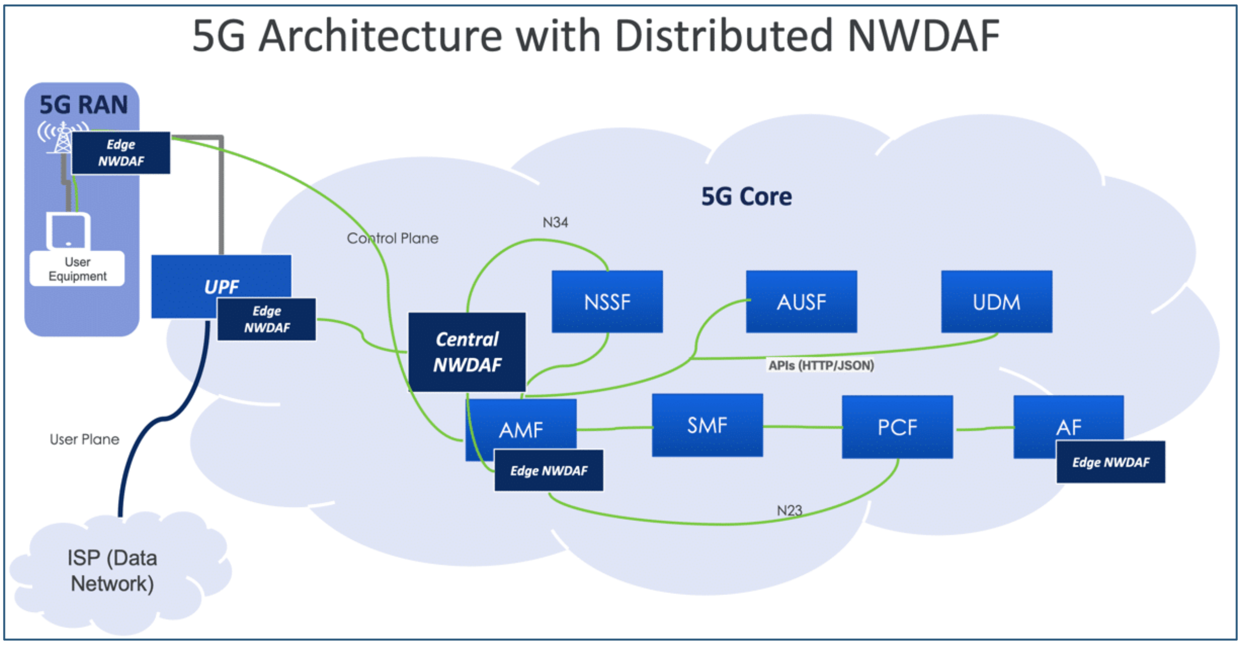
Network Exposure Function (NEF) plays a critical role for 3rd Party Applications and Partners

NEF plays a key role in linking external B2B and B2B2X *Application Functions* (AFs) with the relevant NFs so they can, in real time, configure and deliver products and services over the 5G *Business Bridge*. The 'Bridge' allows CSPs to create the real-time technical bonding that permits trusted 3rd. parties to define, create, deploy and monetize services for a wide variety of innovative applications – many not yet even defined by 3GPP. NEF enables both internal and external applications to safely access capabilities of the 5G *Functional Plane* and facilitates ***secure, robust, developer-friendly access to specified network services and capabilities under the control of a multi-layer policy framework***. The CSP *Value Plane* provides these 3rd parties and business partners a complete monetization environment including the *digital Business Support System* (BSS) – at the top of the chart – including the Product Catalog, Billing processes, Wholesale and Network-as-a-Service (NaaS) facilitation, Customer Care and Partner Management.

Distributed Network Data Analytics Function (NWDAF) offers critical inputs for Enterprise Edge and Cloud Partners

For Private Enterprise Networks and Edge Cloud, a distributed NWDAF can play a key role either for *near real-time analytics at the Enterprise edge or for analytics that require multi-source aggregation and processor intensive statistical analysis* e.g. to *feed a central CSP or HCP managed service location with data* for End-to-End (E2E) service experience analysis. The chart below shows a typical topology for the deployment of a Distributed NWDAF.

Chart C. Example of NWDAF deployment at the Edge and Centrally



Source ***TMForum Insight*** *June 2020*

III. How Network Functions Enable Service Revenues for: *Network Slicing, Cloud Enablers, Edge Services and User Configurable Services*

To leverage these Network Functions for specific revenue generating services we need to map potential new services to the relevant functionality that NEF and NWDAF can provide. *Note: In most cases several other Network and Service Functions are also required to complete a service use case.* Below we identify six **potential NEF and NWDAF enabled services** that contribute to four of the most important 5G revenue generating service categories as follows:

Network Slicing

- ***Service 1:*** **Dedicated Secure Private VPN Management and Exposure of new 5G capabilities**
- ***Service 2:*** **Dynamic Virtual Private Slice Prioritization, Monitoring and Automation**
- ***Service 3:*** **Managed/Shared Slice Handling and Resource Allocation**

Cloud Enablers

- ***Service 4:*** **Cloud Flexibility**

Edge Services

- **Service 5: Edge Resource Allocation and Scaling**

***User Configurable Services on Demand** – the original 'NFV Dream'*

- ***Service 6:*** **Service Function Chain Selection** - *'Service Configuration as a Service'*

NEF and NWDAF each provide capabilities for the four emerging services
Network Slicing, Cloud Enablers, Edge Services and ***User Configurable Services*** as described below.

Network Slicing

Network Slicing has often been touted as a critical 5G revenue generator. But it depends on configuration and dynamic orchestration to assure End-to-End (E2E) service quality across multiple domains as described in the new Amdocs sponsored white paper on '*New Approaches Address End-to-End Network and Service Orchestration (E2ENSO) Challenges*'[6]. NEF plays a key role in defining the E2E Service Functions (SFs) that are authorized to form the Service Function Chains (SFCs) within each Network Slice type to create a guaranteed service. Network orchestration capabilities that instantiate, manage and operate these network slices across multiple technology, network and cloud domains then play a critical role in monetizing underlying network functionality.

For *Network Slice based 'Private VPNs'* NEF can ensure E2E functional isolation for privacy and security that has historically been delivered through separate physical connectivity or router controlled VPNs. In conjunction with Policy Control Function (PCF), Session Management Function (SMF) and Network Resource Function (NRF), NEF can limit secure real time applications access to the specific authorized secure private Service Functions at the core or at the edge e.g. for Drones performing multiple services – Surveillance, Video Streaming, Package Handling etc.

As Chart B showed the E2E Orchestration platform provides Life Cycle Management (LCM) with support for the *Business Bridge* and the *Value Plane* including the E2E network and service assurance that makes Network Slicing possible. *Dynamic Virtual Private slice prioritization, monitoring and automation and managed/shared slice handling with dynamic resource allocation all critically depend on E2ENSO.*

Within the E2ENSO framework:

NEF enhances Network Slicing by enabling:

- *Secure Edge Access Validation and Privacy*
- *Custom Slice Configuration Exposure and Selection*
- *Support for future Slice Configuration as a Service*

NWDAF assures Network Slicing with inputs for:

- *Managed Network as a Service (NaaS)*
- *SLA performance Visibility*
- *Monitoring Dynamic Slice Assignment and Orchestration*

Feeding performance data from the NWDAF into the E2E 5G slicing orchestrator enables operators to assure 5G slicing operations and E2E slice assurance, as well as supporting optimization of network function 'homing' and 'placement', closed loop automation, UE traffic optimization and mitigation of network slice congestion.

Cloud Enablers

Cloud Enablers are NEF capabilities that support *Secure Edge Cloud Access* and *Edge Storage and Compute Instance Activation.* NEF enabled *Secure Edge Cloud Access control* complements Cloud Hyperscaler security at the edge, by providing pro-active security authorization or pre-emptive blocking for threats to 'Edge Cloud' Apps, and compute and storage resources. Traditional IT firewalls are often too cumbersome to be deployed at the edge and *often internet security operates only after penetration has occurred, and the network or service platforms are already under attack.*

The economics of deploying resources in the 'Edge Cloud' are very challenging for both CSPs and HCPs since the 'law of small numbers' may leave edge compute and storage resources underutilized as 'stranded assets' or worse - inadequate to handle highly variable peak loads. The key to profitable and reliable edge services is *Edge Storage and Compute Instance Activation* that dynamically triggers active instances of an application or NF in milliseconds (ms) on the 'nearest' logically adjacent network servers – based on distance and topology based latency constraints. Dynamic storage and compute resource monitoring and activation across a metro-area is key to Hyperscaler 'Edge Cloud' resource management outside the Data Center.

NWDAF enables *Multi-Cloud Monitoring* and *Load Tracking* that are essential for Dynamic Storage and Compute including Load Balancing across Data Centers, across a Metro Area or at the edge. It can play a key role in monitoring and management of both CSP network traffic and HCP workloads and can provide critical support for services that require *Cloud Flexibility* and *Edge Resource Allocation or Scaling.*

Edge Services

Edge Services create a unique opportunity to offer new CSP value. Applications - in this context *Application Functions* (AFs) - are increasingly deployed '*at the edge'* of a CSP network or an HCP 'Edge Cloud' running on a Commercial Off the Shelf (COTS) server platforms. They may be co-located with Radio Access Network (RAN) baseband signal processing e.g. an O-RAN Distributed Unit (DU), instantiated at the edge with *Multi-Access Edge Compute* (MEC) or on a remote server connected to centralized 5G core processors. Such distributed servers, however, offer a large 'attack surface' for hackers and potential network intruders. Yet Edge processor resources are often insufficient to support traditional IT or Internet security software. A new approach is needed.

The NEF can help here by playing a critical pro-active '*gatekeeper*' role to secure access at the edge and determine which trusted Apps are allowed to access specific NFs and network resources – before they become a threat. It builds on **5G SA's inherent security design and authentication functions to pre-emptively block Distributed Denial of Service (DDoS) attacks and pre-emptively block threats at the edge**. NEF is also a key enabler for high performance, low latency and massively scalable 5G services - eMBB, URLLC, mMTC etc. For example, if an external AF requires low latency communication services such as *interactive gaming* or *near real time industrial production monitoring*, the NEF provides safe and secure API invocations for the AFs and orchestrates the API call to the relevant 5G Core NFs, so that together they deliver the requested Class and Quality of Service (QoS) to the Edge service or *User Equipment* (UE)/mobile device, over the *User Plane Function* (UPF) to the *Application Function* servers – wherever they may be.

NWDAF can also play a **major role in optimizing distributed processing and storage for Edge Services across many small, scattered locations** as it captures the necessary inputs for distributed load balancing across these diverse edge resources and feeds that data directly to a Machine Learning (ML) engine or AI algorithm – often itself on an Edge server - to enable real time traffic analysis and optimization and dynamic resource allocation. To summarize:

At the Edge NEF supports:

- *Secure Edge Validation and Privacy*
- *Secure Edge Cloud Access*
- *Edge Storage and Compute Instance Activation*

At the Edge NWDAF captures data for:

- *Edge Services Monitoring*

And provides essential inputs for:

- *New Physical Instance activation*
- *Storage and Compute with Load Balancing at the edge*
- *Redirection of Edge Traffic o*
- *Edge Service Recovery based on Policy Rules*

User Configurable Services

User Configurable Services are the ***original 'NFV Dream'*** and began with *Slice Configuration as a Service* and evolved to *User Managed Slice Configuration on Demand*

These NEF assisted use cases are a precursor to *Service Function Chain (SFC) selection or 'Service Creation/Configuration as a Service'*. 'On demand SFC selection' will one day leverage Policy Control and NEF to ***allow trusted customers to select not only bandwidth and latency parameters but also the combination of Service functions that make up an SFC that they require*** e.g. for remote control for different classes of robots or vehicles. *Note: SFCs will always need to be configured, tested and authorized by CSPs in advance to minimize any potential 'harm to the network'.*

Based on their trustworthiness and administrative status, peer operators, MVNOs, Enterprise customers, Cloud Hyperscalers and 3rd party software partners should all eventually be able to modify and customize different flavors of the same service as customized SFCs.

NWDAF enables User Configurable Services to be validated and monitored as part of *Bandwidth and Service Features 'On Demand'*. While other functions manage and instantiate the SFs for any on demand SFC, the NWDAF provides critical intermediary inputs for monitoring and analysis of any anomalies is the functioning of these flexible services before they cause network problems.

IV. Opportunities for Services vary by User/Customer

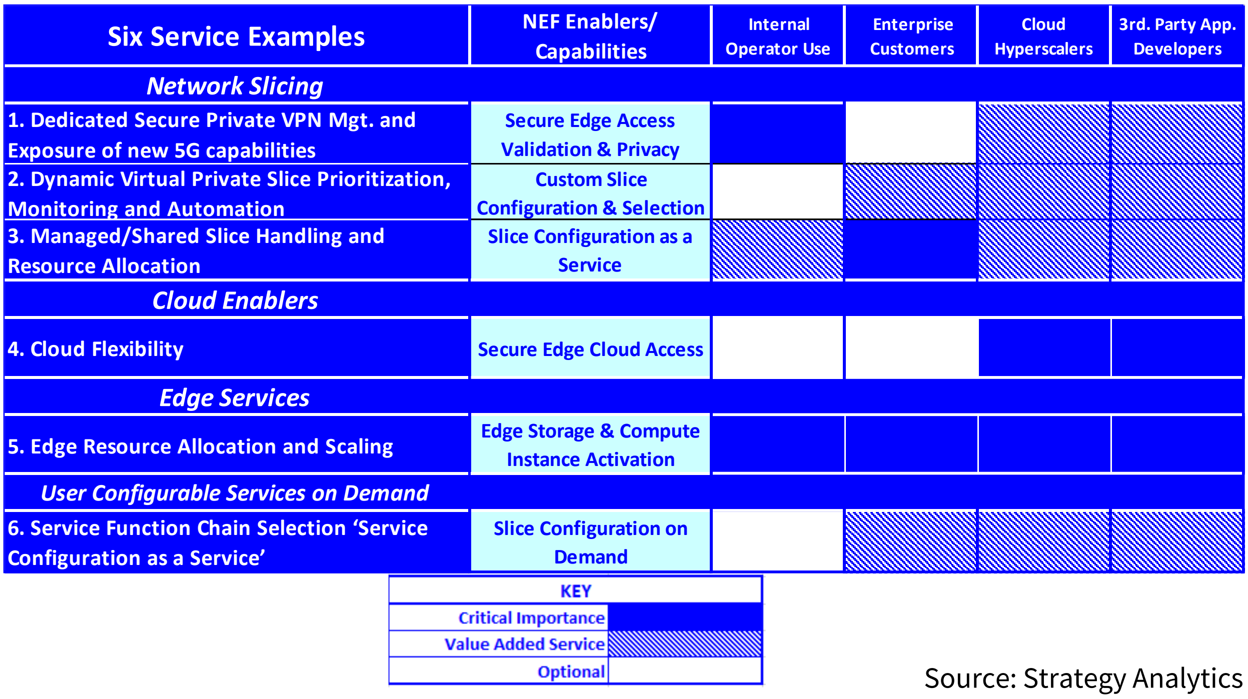
The two charts below summarize the likely importance of opportunities for the four service categories described above and the relative importance of each opportunity for:

- **Internal Operator Use**
- **Enterprise Customers**
- **Cloud Hyperscalers**
- **Third Party App. developers**

IV.1 NEF Service Opportunities for four different Types of Users/Customers

Service examples are listed in the leftmost column. Potential and related capabilities – or the role of NEF/NWDAF to deliver the service - are listed in the second column. The rightmost four columns indicate the likely opportunity by type of user or customer i.e. Internal Operator Use, Enterprise customers, Cloud Hyperscalers or 3rd party application developers.

Chart D. Opportunity for NEF assisted Service Features to Different Users/Customers



Six Service Examples	NEF Enablers/ Capabilities	Internal Operator Use	Enterprise Customers	Cloud Hyperscalers	3rd. Party App. Developers
Network Slicing					
1. Dedicated Secure Private VPN Mgt. and Exposure of new 5G capabilities	Secure Edge Access Validation & Privacy	■	□	▨	▨
2. Dynamic Virtual Private Slice Prioritization, Monitoring and Automation	Custom Slice Configuration & Selection	□	▨	▨	▨
3. Managed/Shared Slice Handling and Resource Allocation	Slice Configuration as a Service	▨	■	▨	▨
Cloud Enablers					
4. Cloud Flexibility	Secure Edge Cloud Access	□	□	■	■
Edge Services					
5. Edge Resource Allocation and Scaling	Edge Storage & Compute Instance Activation	■	■	■	■
User Configurable Services on Demand					
6. Service Function Chain Selection 'Service Configuration as a Service'	Slice Configuration on Demand	□	▨	▨	▨

KEY	
Critical Importance	■
Value Added Service	▨
Optional	□

Source: Strategy Analytics

As the Chart above indicates, different groups of customers will be attracted to different NEF enabled services as described below.

a. Internal Operator Use. Operators are most likely to focus on capabilities for their immediate Internal use that allow them to deliver Private and Virtual Private Networks (VPNs) over Wireless – much as they have been doing for many years over Fixed Networks. *Dedicated Secure Private VPN Mgt. and Exposure of new 5G capabilities* will therefore be most useful to operators internally for segregating and orchestrating Private Network services and for 'Dedicated Access' over Fixed (Wired, Wi-Fi) and Mobile transport.

Operators will also be very interested in *Edge Resource Allocation and Scaling* features that allow them to dynamically allocate and scale scarce resources, as the Edge Services market accelerates in late 2021.

b. Enterprise Customers. Many large corporate enterprises will probably be slow to switch to a 5G virtual service like *Dynamic Virtual Private Slice Prioritization, Monitoring and Automation* or to move away from their current dedicated fixed MPLS VPNs and SD-WAN services. Over the next two years, however, some will begin to gain confidence in the **inherent security, privacy, adaptability and reliability of 5G,** and begin to adopt truly virtual Network Slicing.

Small and Medium Enterprises (SMEs), however, are most likely to be more immediately interested in getting *Managed/Shared Slice Handling* services as 5G SA creates a new market for 'Virtual Managed VPNs' at a price point that attracts these new business users to services they have previously been unable to afford.

c. Cloud Hyperscalers and ***d. 3rd Party App. Developers*** will both likely be interested in NEF capabilities for *Cloud Flexibility* and *Edge Resource Allocation and Scaling* in 2021.

Select Enterprise Customers and Vertical Industry App. Developers will begin to experiment with *Service Function Chain Selection i.e. 'Service Configuration as a Service'* for special vertical or unique applications that require multiple feature variations and where '*custom pre-configuration'* of SFCs is paid for. These could include applications for remote controlled UEs such as Drones – for 'Swarm' Control, Drone Video Capture or Drone Imagery for 'Heads up Displays' of burning buildings superimposed on floor plans for firefighters etc. However, there are likely to be many experiments before there is widespread deployment of '*Service Configuration as a Service'* – a service that could be called the '***NFV Dream'* of configurable service features on demand.** Widespread adoption is probably still several years away beyond 2023.

Near Term NEF Opportunities

In the near term the most important opportunities for NEF assisted revenue generating services are therefore expected to be as follows:

Cloud Flexibility delivered to Cloud Hyperscalers or working with 3rd Party App. Developers to integrate Cloud Native IT services 'at the edge' and Apps. for vertical markets that require Cloud Hosted Extranets e.g. Supply Chain and Logistics

Edge Resource Allocation and Scaling where CSPs bring unique security and load management capabilities to the edge services market and complement the Cloud Hyperscalers with network intelligence, real time control of distributed resources and pre-emptive security.

IV.2 NWDAF Service Opportunities for four different Types of different Users/Customers

The Chart below shows the estimated opportunities for NWDAF enabled services. Below we discuss the likely importance by User/Customer group.

Chart E. Opportunities for NWDAF Service Features to Different Users/Customers

Six Service Examples	NWDAF Enablers/ Capabilities	Internal Operator Use	Enterprise Customers	Cloud Hyperscalers	3rd. Party App. Developers
Network Slicing					
1. Dedicated Secure Private VPN Mgt. and Exposure of new 5G capabilities	Managed 'NaaS', Private Network Monitoring	■	■	▨	■
2. Dynamic Virtual Private Slice Prioritization, Monitoring and Automation	CIO SLA Visibility	▨	■	□	□
3. Managed/Shared Slice Handling and Resource Allocation	Dynamic Slice Assignment and Orchestration	■	▨	▨	▨
Cloud Enabler					
4. Cloud Flexibility	Multi-Cloud Monitoring & Load Redirection	▨	■	■	■
Edge Services					
5. Edge Resource Allocation and Scaling	Storage and Compute Load Balancing at the Edge	■	▨	■	■
User Configurable Services on Demand					
6. Service Function Chain Selection 'Service Configuration as a Service'	Bandwidth and Service Features 'On Demand'	▨	■	▨	▨

KEY	
Critical Importance	■
Value Added Service	▨
Optional	□

Source: Strategy Analytics

a. Internal Operator Use. For NWDAF the best Internal Operator use cases are those that support ***Network Slicing*** and ***Edge Services*** – two critical high growth pre-5G and 5G markets. NWDAF enhances *Dedicated Secure Private VPN Mgt.* with NaaS and Private Network Monitoring and Assurance, while for *Managed and Shared Slice Handling* it enables Dynamic Slice Assignment and Orchestration. Operators are also likely to prioritize the use of NWDAF inputs to enable *Edge Resource Allocation and Scaling* with Storage and Compute with Load Balancing 'at the edge'.

b. Enterprise Customers are likely to have significant near term interest in the NWDAF enabled capabilities for service examples that relate to user and CIO visibility through control of network monitoring and private as well as cloud based SLA visibility.

c. Cloud Hyperscalers and **d.** ***3rd party App. Developers*** are most likely to be interested in *Cloud Flexibility* and *Edge Resource Allocation and Scaling* just as in in the NEF Opportunity Chart D (above).

V. Summary of Business value of Selected Services by User/Customer Type

To assess the value of the selected services that leverage NEF and NWDAF, we created the Chart below to summarize service value for of the four User/Customer categories - Operators, Enterprises, Cloud Hyperscalers and App. Developers. Appendix C provides a text summary.

Chart F. NEF and NWDAF come together to create enhanced business Value for the six services in each of the Customer Markets

New Service Examples	Contributing NF	NEF /NWDAF Capability	*Value Bridge*	Internal Operator Value/Savings	Enterprise Service Value	Cloud Hyperscaler Value	App. Developer Value
1. Dedicated Secure Private VPN Mgt. and Exposure of new 5G capabilities	*NEF*	Secure Edge Access Validation & Privacy	Together	Revenue for High Value 'Inherently Secure' Private Networks	Dedicated Private Network Privacy at Shared Public Network Price	No Firewalls needed for Edge Cloud Servrices	Apps simpler and faster to build since Netrwork provides Security
	NWDAF	Managed 'NaaS', Private Network Monitoring					
2. Dynamic Virtual Private Slice Prioritization, Monitoring and Automation	*NEF*	Custom Slice Configuration & Selection	Together	Reduced Ops. Costs for Flexible Services and Network Slicing	CIO Power to Control Network Service Quality and Monitor SLAs	Resell Configurable Service for Hosted Enterprise Customers	Wide Variety of Apps. get only the Priority they need
	NWDAF	*CIO SLA Visibility*					
3. Managed/Shared Slice Handling and Resource Allocation	*NEF*	Slice Configuration as a Service	Together	Shared Network Slicing becomes Manageable and Profitable	Both On-Demand Band-width and On-Demand Shared Slices	Turnkey Service Domains for Verticals or Apps. W. same QoS	Easy to develop Re-usable Software for *Groups of Similar Verticals* or *QoS Slices*
	NWDAF	*'Dynamic Slice Assignment' and Orchestration*					
4. Cloud Flexibility	*NEF*	Secure Edge Cloud Access	Together	Telco. maintains Control of Hybrid Cloud Market	Enterprise can monitor Hybrid Public Private Multi-Cloud	Hyperscaler can offer full visibility of Network Connectivity	Northbound Network APIs makes Resource allocation transparent for Developer
	NWDAF	*Multi-Cloud Monitoring & Load Redirection*					
5. Edge Resource Allocation and Scaling	*NEF*	Edge Storage and Compute Instance Activation	Together	Reduced Risk of 'Stranded Assets' at the Edge	Edge Cloud can operate 'On Premise' or have network backup	Cloud Edge Zones can leverage Network Event Info. & Status	Easy to develop Apps for Groups of Similar Verticals or QoS Slices
	NWDAF	*Storage and Compute Load Balancing at the Edge*					
6. Service Function Chain Selection 'Service Configuration as a Service'	*NEF*	Slice Configuration on Demand	Together	Revenue from Variable Service Creation	Enterprise can turn Service Features on or off	Hyperscalers can bundle Telco Services 'as their own'	Dramatically reduces Time to Market for New Service Features
	NWDAF	*Bandwidth and Service Features 'On Demand'*					

Source: Strategy Analytics, Network and Platform Services

VI.Implications

This report has described significant opportunities for CSPs to leverage Network Functionality based on NEF and NWDAF for new CSP revenue generating services, that add value to Enterprise customers, HCPs and their App. Developers with significant new service capabilities.

Key 'Take Aways'

CSPs should take away from this report just how important NEF and NWDAF could become important Network based 'Value Creators' for Operators themselves and their friendly Cloud competitors.

NEF and NWDAF are important Value Creators' for CSPs

NEF and NWDAF create value as they enable CSPs to:

- Turn Network Functionality into Service Revenues
- Share Slice Configuration and Service Management securely with Trusted Customers and Partners
- Translate Network Events and 'Metadata' into Analytics and Service Value
- Provide predictive insights to optimize resource utilization efficiency – especially at the edge
- Leverage Network Analytics to ensure Service Level Agreements (SLAs) are never violated
- Use Network and Service usage patterns to provide sophisticated Service recommendations and offers
- Adopt ML and AI to enhance critical decisions and enable closed loop automation
- Provide User Interface (UI) to give Enterprise CIO visibility and control over both the QoS and Service Features they activate on any Network Slice
- Provide Cloud Hyperscalers with both Network and E2E Service Monitoring in near real time
- Offer 3rd party Developers secure access to Northbound APIs for authorized Service Functions

Importance of the Service examples

The four categories of services reviewed in this report will be among the most significant 5G SA Revenue generators in the long run. They are ***Network Slicing, Cloud Enablers, Edge Services*** and ***User Configurable Services***. Each of the four critically depends on the network based capabilities enabled in part by NEF and NWDAF functionality and summarized below:

- ***Network Slicing*** depends on *inherent 5G Security and Privacy mechanisms* to avoid commoditization while achieving 20 – 30 percent savings from *Virtualization and Dynamic Resource Management*.
- ***Cloud Enablers*** depend on *Dynamic Compute* and *Storage Allocation* 'at the edge' and across the metro area to create a 'Telco Connectivity Cloud' that adds significant value to the Hyperscaler's 'Data Center Cloud'
- ***Edge Services*** rely on Carrier Class response times with single digit milliseconds (ms) for Control Plane and Service event responses to assure performance for low latency Apps. and state aware instantaneous recovery – in contrast to Round Trip Times (RTT) of 200 ms and potential packet loss in the 'Best Effort' Public Cloud
- ***User Controlled Service Options and Policies*** will eventually evolve to allow user or CIO configuration of ***Service Function Chaining on Demand*** – a truly cloud native hyper scalable service.

While the example services described in this report may *not look like the traditional end user 'Killer Apps' that CSPs continuously seek and rarely find*, they are all likely to generate significant revenue as enablers for CSP managed Private Networking, Cloud and Edge services as well as 3rd Party Vertical industry solutions. These services are likely to be very 'sticky' as they become embedded in Enterprise and HCP solutions and can be expected to grow in value as part of those customers' own digital transformation. CSPs can in turn expect these capabilities to translate to enhanced revenues and margins for themselves through 2026.

References

1. '**Network Exposure Function - The Next Phase of 5G'**, Telecoms.com Webinar, July 2021

2. '**Management, Orchestration & Automation not just Overhead anymore**', Strategy Analytics Insight, November 2019

3. '**5G Service Based Architecture (SBA) - Design Principles**', Strategy Analytics Report, April 2019

4. '**Pricing, service and partner innovation in 5G**', TM Forum March, 2021

5. '**NWDAF: Automating the 5G network with machine learning and data analytics**', TMForum Insight. June 2020

6. '**New Approaches Address End-to-End Network and Service Orchestration (E2ENSO) Challenges'**, Strategy Analytics, July 2021

7. '**A House Divided: Dysfunctional Relationships Between Network and Cloud Teams Put Cloud Strategies at Risk**' Sponsored by **Blue Cat Networks** EMA Custom Research Report, April 2021

8 '**Network Exposure: Opening up 5G networks to partners**' Openet Blog, May 2020

9. **'Network Exposure Function (NEF) – Built for 5G'**, Openet Data Sheet

10. '**Network Data Analytics Function (NWDAF) – Built for 5G Data Insights**', Openet Data Sheet

Analyst Contact

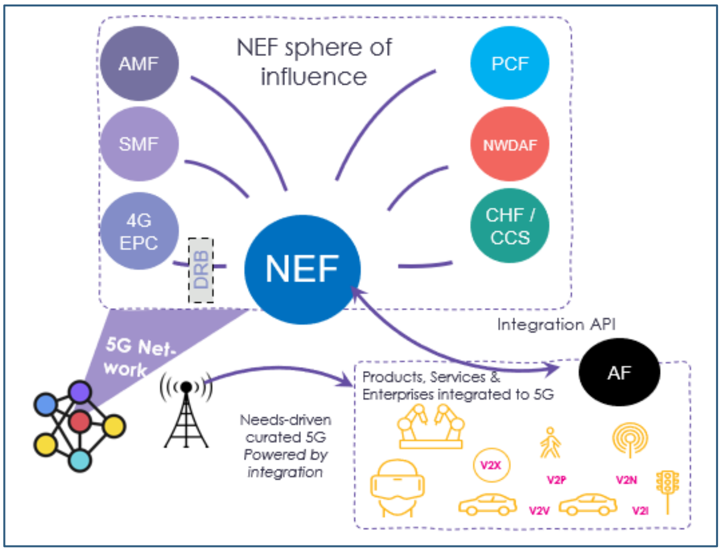
The author of this Report: Sue Rudd, Director Networks and Service Platforms at Strategy Analytics can be reached at **srudd@strategyanalytics.com**,

Appendix A. Network Exposure Function (NEF) Description

NEF can act as an Intermediary or 'Gateway' that controls and arbitrates 3rd Party Access

NEF enables and controls secure access to exposed network or service functions via a set of northbound RESTful (or web-style) APIs to both internal - i.e. within the network operator's trust domain - and external application/partner domains. Southbound Network Interfaces allow flexible integration with both 4G functions (using Diameter) and 5G via 5G SA Service-Based Interface (SBI). Authorized 3rd party developers and enterprises can use the available Northbound APIs to create their own network services on-demand. Service Assurance and Network Automation can be *"enhanced by application server interactions with policy and charging controls as well as network analytics, edge computing components and network slicing. The NEF can provide a multi-layer policy framework that enables policy decisions at the application, business and infrastructure levels."* See: Blog[8].

Chart A1. Network Exposure Function has a key 'Sphere of Influence'



Source: Openet Division of AMDOCS, NEF Data Sheet[9]

NEF provides real time control of service function visibility for the Session Management Function (SMF) and the Access and Mobility Function (AMF) to enable domain specific control for authorized Application Functions (AFs) based on Policy Control Function (PCF) rules, with Charging options via Charging Function (CHF) and NWDAF analytics. NEF capabilities can be applied to multiple 5G application domains as shown at the bottom right e.g. for Robotics, V2X etc.

NEF is Intermediary for Inherently Secure Network and Service Function Access

NEF can be viewed as the '*Gatekeeper'* function of 5G that determines which Network Functions (NFs) and Service Functions (SFs) can interact with other specifically authorized NFs and SFs. Any Service Function (SF) that NEF is not authorized to expose - by Policy, Session Management and Network Resource Functions - is *not even visible* to the requesting unauthorized SF. NEF operates in the same way to allow both internal and authorized 3rd party Application Functions (AFs) to access operator SFs so that for example 3rd party software developers can create new Apps. via the available Northbound API for each SF. The Network Exposure Function acts as an intelligent, service-aware 'border gateway' that enables external AFs to communicate with the 5G SA Network Functions.

Appendix B. Network Data Analytics Function (NWDAF) Description

NWDAF provides enhanced intelligence for Network Decision Making

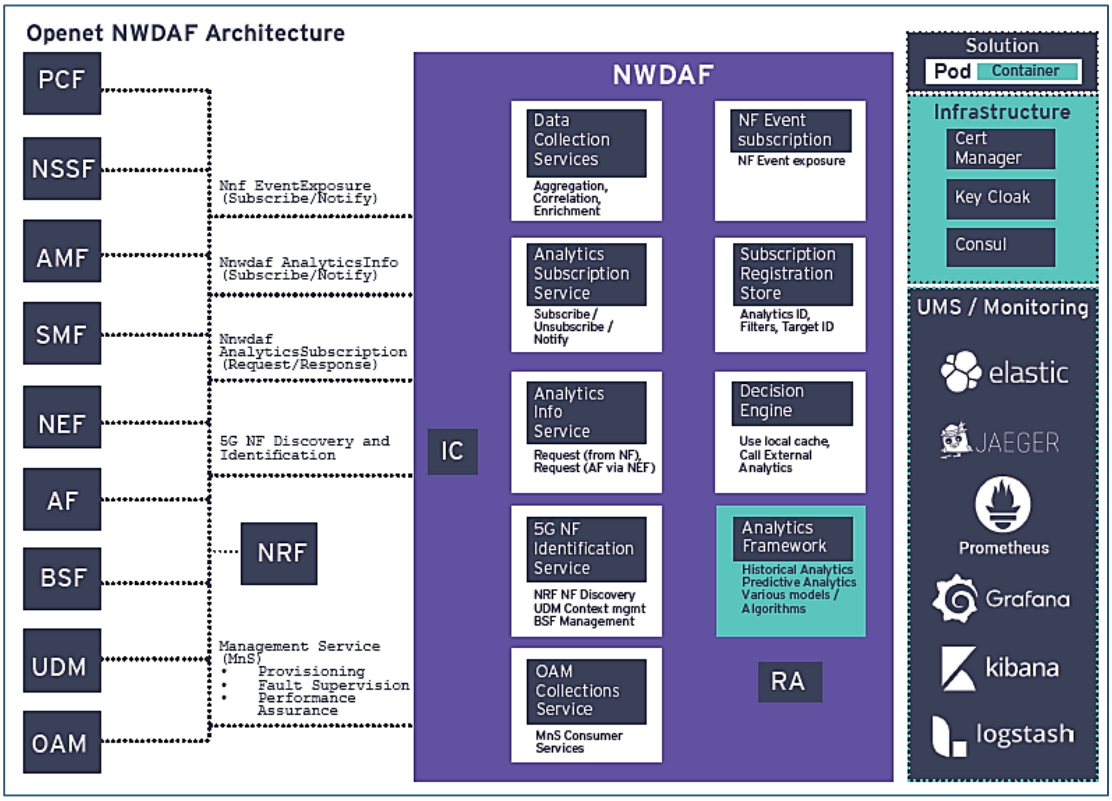
NWDAF collects data from multiple other Network Functions (NFs) and procedures using a subscription/ request model to provide access to statistics and predictions for applications that *optimize resource utilization, evaluate quality of experience* or *provide insight to Network Operations* for key network decisions. NWDAF provides critical input for:

- Closed Loop Automation based on Analytics, AI and Policy to automate network and service optimization.
- Efficient monitoring of QoS and SLA compliance
- Auto-Discovery to enable creation of new services
- Network Slicing to offer features on a per network slice basis
- Monetization of 5G Network and Service Functions.

NWDAF leverages predictive algorithms and enables enhanced decision making

The **main components of NWDAF Architecture** are shown in the Chart below. NWDAF Core is responsible for collecting data from the network and for exposing interfaces. The Open Data Fabric (ODF) enables data interchange, persistence and querying, and *Machine Learning (ML) processes data inputs to create, train and manage models of network traffic and event prediction* etc.

Chart B1. AMDOCS Openet NWDAF leverages Nine Modules to supports Solutions for K8s Pods/Containers, Infrastructure and Unified Messaging System (UMS)/Monitoring



Source: Openet Division of AMDOCs, NWDAF Data Sheet[10]

As the chart above shows the NWDAF collects, aggregates, analyses and models events and data from all the Network Functions shown on the left – *Policy Control Function* (PCF), *Network Slice Selection Function* (NSSF), *Access and Mobility Function* (AMF), *Session Management Function* (SMF), *Network Exposure Function* (NEF), *Application Function* (AF), *Binding Support Function* (BSF), *Unified Data management* (UDM), *Operations, Administration and Maintenance* (OAM) and *Network Resource Function* (NRF).

NWDAF therefore captures in almost real time across the network infrastructure, the level and types of events and activity of every major Network Function. These are often referred to as 'Metadata' i.e. data associated with delivery and operation of services but *not the service content itself*. Analytics and Machine Learning are then applied to the data presented by the NWDAF to create both statistical profiles and predictions of network activity.

NWDAF is the 'Stethoscope' that monitors and amplifies the beating heart of the CSP's network.

NWDAF AI/ML Use Cases

3GPP TR 23.791 has listed the following formula-based/AI-ML analytics use cases for 5G using NWDAF:

- Load-level computation and prediction for a network slice instance
- Service experience computation and prediction for an application/UE group
- Load analytics information and prediction for a specific NF
- Network load performance computation and future load prediction
- User Entity (UE) Expected behavior prediction
- UE Abnormal behavior/anomaly detection
- UE Mobility-related information and prediction
- UE Communication pattern prediction
- Congestion information – current and predicted for a specific location
- Quality of Service (QoS) sustainability which involves reporting and predicting QoS change

Appendix C. Summary of Business Value Proposition for Operators, Enterprises, Hyperscalers and App. Developers.

Chart F. in Section V. of the main report indicates that putting both NEF and NWDAF Network Functions together – in conjunction with other relevant Service Functions - will provide significant value for ***Operators, Enterprises, Hyperscalers*** and ***App. Developers*** both in the near term and over the next five years.

Below is a convenient summary of the business value propositions for each group based on Chart F.

The numbers 1 through 6 refer to the associated *six service examples described in Section III of the main report.*

a. Internal Operator Value/Savings for the six services come from:

1. Revenue for High Value 'Inherently Secure' Private Networks
2. Reduced Operations Costs for Flexible Services and Network Slicing
3. Shared Network Slicing that becomes Manageable and Profitable
4. Telco. control of Hybrid Cloud access for Enterprise
5. Reduced Risk of 'Stranded Assets' at the edge
6. New Revenues from configurable Service Function Chain Creation

b. Enterprise Service Value comes from:

1. Dedicated Private Network Privacy at Shared Public Network Price
2. CIO Power to Control Network Service Quality and Monitor SLAs
3. Both On-Demand Bandwidth and On-Demand Shared Slices
4. Enterprise can monitor Hybrid Public Private Multi-Cloud
5. Edge Cloud can operate 'On Premise' or have Managed Network backup
6. Enterprise can turn Service Features on or off

c. Cloud Hyperscaler Value derives from:

1. No Firewalls needed for Edge Cloud Security
2. Ability to Resell Configurable Service for Hosted Enterprise Customers
3. Turnkey Service Domains for Verticals or Apps. with same QoS
4. Hyperscaler can offer full visibility of Network Connectivity
5. Cloud Edge Zones can leverage Network Event Info. & Status in near real time
6. Hyperscalers can bundle Telco Services 'as their own' i.e. “White Label’

d. 3rd Party and Vertical Industry App. Developer Value is created because:

1. Apps. are simpler and faster to build since Network provides multiple Northbound APIs and Security
2. Wide Variety of Apps. request and receive only the Priority they need
3. Easy to develop re-usable Software for *Groups of Similar Verticals* or *QoS Slices*
4. Northbound Network APIs available to make Resource allocation transparent to the developer (and end user or Enterprise)
5. Easier to optimize Apps. for Groups of Similar Verticals or QoS Slices
6. Dramatically reduces Time to Market for new Apps. and Service Features

Get help from Strategy Analytics

Working with Strategy Analytics gives you the knowledge you need to succeed.

Understand your customer

Business opportunities abound. But which ones are right for you and your customers? Which will give you the advantage?

Optimize your user experience

Optimize your product to give your users the best experience and you the market advantage.

Analyze the market

Understand the size of the opportunity and where your product fits using our unrivalled knowledge and world class data analysis techniques.

Explore your future

Working with us will focus you. With our insight and forecasting expertise you'll make confident strategic decisions that drive success.

Please contact us at **custom@strategyanalytics.com** with any questions and for further details and solutions on how we can work with you on creating a custom solution to address your specific needs.