TeckNexus
DIGITAL SERVICE PROVIDER ECOSYSTEM

Whitepaper prepared for RADCOM

WHY YOU NEED A NEW APPROACH TO ASSURANCE FOR 5G NETWORKS?

RADCOM

2020 | November

Prepared by Hema Kadia | TeckNexus

CONTENTS

EXECUTIVE SUMMARY

5G networks began rolling out about a year ago. As of mid-sept 2020, there are 98 live commercial 5G deployments in 49 countries, as tracked by TeckNexus.[1]

Globally, 5G operators have already started delivering on industrial use cases leveraging ultra-low latency and multi-access edge computing and a wide range of consumer apps leveraging AR/VR & wearables.

To ensure that the operators deliver on the service quality and the SLAs promised to the enterprises and consumers, they need assurance solutions that seamlessly integrate within their complex hybrid network and enable their network to self-optimize.

In TeckNexus's view, the assurance solutions need to adopt a new approach such as cloud-native technologies and architecture to ensure the 5G networks & the related use cases.

3GPP is already pushing towards adopting cloud-native technologies with Service Based Architecture (SBA) in Release-15 and enhancement to Service Based Architecture (eSBA) in Release-16.

European Telecommunications Standards Institute (ETSI) has also adapted the NFV reference architecture to support the Cloud Native Network Functions (CNFs).

To ensure this cloud-native 5G network & ecosystem, it becomes imperative for assurance solutions to adopt a new approach and cloud-native technologies.

This white paper covers critical requirements, technologies, and approaches that assurance solutions must support to ensure 5G networks.

ASSURANCE: A LOOK BACK & LOOK AHEAD

Communication Service Providers (CSPs) need to have complete visibility into their network to understand the service quality and the customer experience they provide to their customers.

To gain network visibility, CSPs | network operators deploy service assurance solutions that monitor the network traffic and provide actionable, contextual insights into network performance and the customers' quality of experience.

Service assurance solutions also offer the ability to proactively and reactively troubleshoot issues, allowing CSPs to maintain top-level service quality and keep customer experience levels up.

Traditionally, service assurance solutions, like the networks they are monitoring, are composed of expensive, proprietary-owned hardware, static, and deployed as add-ons to the network.

As the network changes, for example, when capacity grows, engineers need to add additional hardware and reconfigure the service assurance solution manually.

Now, as the CSPs are transitioning to the 5G networks, the service assurance solutions also need to be enhanced to support the 5G network requirements for them to continue monitoring the network and ensuring the service quality & customer experience.

WHAT IS NEEDED TO ASSURE 5G NETWORKS ?

01 Full visibility of 5G network

02 High volume monitoring

03 Deciphering encrypted traffic

04 SLAs for slices & services

05 Automation

1: FULL VISIBILITY OF 5G NETWORKS

The complexity of 5G networks has made reliable and thorough monitoring of the network a challenge for operators.

5G network complexity primarily comes from the fact that:

- 5G networks are hybrid, both in the sense that network components of different generations will be operating side by side, especially for incumbent operators
- 5G is composed of traditional physical networks, network functions virtualization, and cloud infrastructure.

Monitoring solutions will need to:

- Ingest multiple data types such as events, EDRs, and packets
- Correlate data from multiple data sources, i.e., from 5G NR to 5G core
- Smart monitoring core networks, network virtualization functions & network edge
- Containerized probe (cProbe) to get high-level & granular level end-to-end network coverage & visibility for critical root cause analysis
- Support both standard packet-based and event-based monitoring
- Complement the smart monitoring based assurance by data from other sources, specifically for containerized microservices
- Support distributed tracing in the network environments to monitor & analyze the cross-process transactions taking place "under the hood."

CLOUD-NATIVE CLOUD-AGNOSTIC

Moving assurance functions to Cloud-Native Functions (CNFs) will enable their deployment & integration anywhere in the complex 5G hybrid network to get full visibility of the network, from RAN to Core.

> ***"RADCOM's automated assurance solution is an important component of the Rakuten Communications Platform, as it allows us to monitor service and subscriber, fulfill analytics on our network performance end-to-end from RAN to Core and IMS, all in a cloud-native virtual environment"***
>
> Tareq Amin
> Chief Technology Officer
> Rakuten Mobile, Inc.

2: HIGH VOLUME TRAFFIC MONITORING

The data volume passing through end-to-end 5G networks, built on entirely new architecture with 5G RAN on top of the 5G core, will be exponentially higher than the LTE networks built on Evolved Packet Core (EPC). Therefore, it is not financially viable to monitor and store all the data going through such networks.

Smart sampling is one of the most efficient and practical approaches. It relies on the policies that define what parts of the networks and what types of data should be the most critical elements to be monitored.

Dynamic sampling is an alternative monitoring approach and should be selected:

- To apply to a higher sample percentage of greenfield networks
- A lower percentage is enough for established networks
- On-demand analytics to be provided when assurance analysts or developers need them
- Provide targeted container-level analytics to isolate & diagnose app failures

Deploy assurance solutions to make full monitoring of the network core, to provide complete visibility of essential services to support SLAs, E.g., services include voice calls, media delivery, and service subscription/unsubscription, all transactions made by key customers.

DEPLOY ON-DEMAND ASSURANCE FUNCTIONS

Cloud-native container-based architecture can collect, process, analyze, index, and store minimal data that doesn't weigh down the network. It can be deployed on-demand to monitor the high traffic volume.

Due to its stateless nature, it will have a low footprint and consume minimal resources.

75%

acceleration in cloud-based workload deployments [2]

66%

reduction in deployment time for new services & functions [3]

3: DECIPHER THE ENCRYPTED TRAFFIC

The network core designed based on Services-Based Architecture (SBA) is typically encrypted using TLS 1.2 or TLS 1.3, thereby encrypting the 5G traffic.

Soon, most traffic will be encrypted, including services like video streaming and gaming.

The encrypted traffic will threaten the service providers' capability to gain full visibility of the data going through their networks, thereby increasing time for root-cause-analysis and repair time, directly impacting the user experience.

> *“With 5G, most traffic will be encrypted, which will pose challenges for operators to get full network visibility.”*
>
> *- Tomer Ilan, Radcom Senior Director of Product Management*

The encryption challenge demands that operators - gather, process, analyze, and correlate data from multiple sources, including network packets, OpenTracing from multiple network interfaces, vendors, and event notifications, to convert data points into insights for operators to deliver optimal customer experience for 5G services.

INTEGRATE MULTIPLE DATA SOURCES (PACKETS & EVENTS)

Correlating a combination of network packets, network events, and Event Data Records (EDRs) will enable operators to collect minimal data from multiple sources while still being able to troubleshoot on-demand when service degradations occur.

~200%

increase in the use of HTTPS (i.e., encryption) for web traffic in the last three years [4]

4: SLA FOR NETWORK SLICES & CRITICAL SERVICES

Network slicing will enable operators to split network resources into logical or virtual networks ("slices") to address specific use cases with distinct characteristics and service level agreement (SLA) requirements.

Operators can allocate the network slices to dedicated services. So, for example, an operator can offer

- Super-fast download times to avid video streamers
- Ultra-Reliable Low Latency Communications (URLLC) to gamers,
- Massive Machine-Type Communications (mMTC) to governments looking to develop smart cities.

Network slicing will open up new revenue channels for the operator.

To ensure that the Service Level Agreements (SLAs) are met corresponding to each network slice, assurance solutions will need to monitor each slice separately and provide insights to verify whether or not the related slice is delivering as per the agreed SLAs.

SCALE WITH THE SLICES

Moving to cloud native will enable assurance solutions to react & ensure that SLAs & Quality of Service (QoS) are met across network slices, including core and RAN network elements, for mission critical services (e.g. emergency services) .

It will also allow them to scale up & down, depending on the capacity needed for specific network slices & services.

70%

of all network issues occur in the RAN, which, if not fixed, can lead to service outages having a critical impact on the customer experience.[5]

5: AUTOMATION

Operators need an automated assurance platform to:

- Manage an exponentially high volume of 5G traffic
- Deploy over public or private cloud infrastructure, containers or virtual machines, bare metal, or any combination of these
- Co-relate data from multiple sources, including packet feeds, event-based feeds from different parts of the network
- Support 3GPP 5G Service-Based Architecture (SBA), including Service-Based Infrastructure (SBI), non-SBI interfaces as well as Control and User Plane Separation (CUPS)
- Efficiently scale leveraging microservices architecture.
- Support containerized orchestration for a closed-loop environment
- Enable automated root cause analysis and anomaly detection to solve network issues in real-time
- Enable journey to self-optimization of 5G networks via closed-loop automation, i.e., feedback of information through the network, which monitors, identifies, adjusts, and optimizes automatically.
- Enable automated service discovery, automatic payload discovery, automated tracing policy configuration, and automated enrichment data discovery

MANAGED BY KUBERNETES

Using Kubernetes will enable operators to automate the deployment, scaling, and management of all containerized functions, delivering a unified view of the network.

The microservices architecture will also allow the operators to update pods instances incrementally with new ones, known as a rolling upgrade enabling deployments with zero downtime.

23%

of Opex is telco's labor costs (Telco's spend approximately **$292 billion** in 2019). Half spent is on the Network and IT Staff.[6]

AUTOMATION IS CRITICAL TO REDUCING COST

KEY TAKEAWAYS

MONITOR THE HIGH VOLUME OF TRAFFIC

Deploy on-demand assurance functions

66% Reduction in deployment time for new services

DECIPHER THE ENCRYPTED TRAFFIC

Integrate multiple data sources

~200% increase in the use of HTTPS for web traffic in the last three years

SLA FOR NETWORK SLICES & CRITICAL SERVICES

Scale with Slices

70% of all network issues occur in the RAN, which, if not fixed, can lead to service outages

AUTOMATION

Managed by Kubernetes

23% Opex is telco's labor costs (Telco's spend approx. **$292 billion** in 2019). Half spent is on the Network and IT Staff

FULL VISIBILITY OF 5G NETWORKS

Cloud-Native | Cloud Agnostic

"RADCOM's automated assurance solution is an important component of the Rakuten Communications Platform, as it allows us to monitor service and subscriber, fulfill analytics on our network performance end-to-end from RAN to Core and IMS, all in a cloud-native virtual environment"

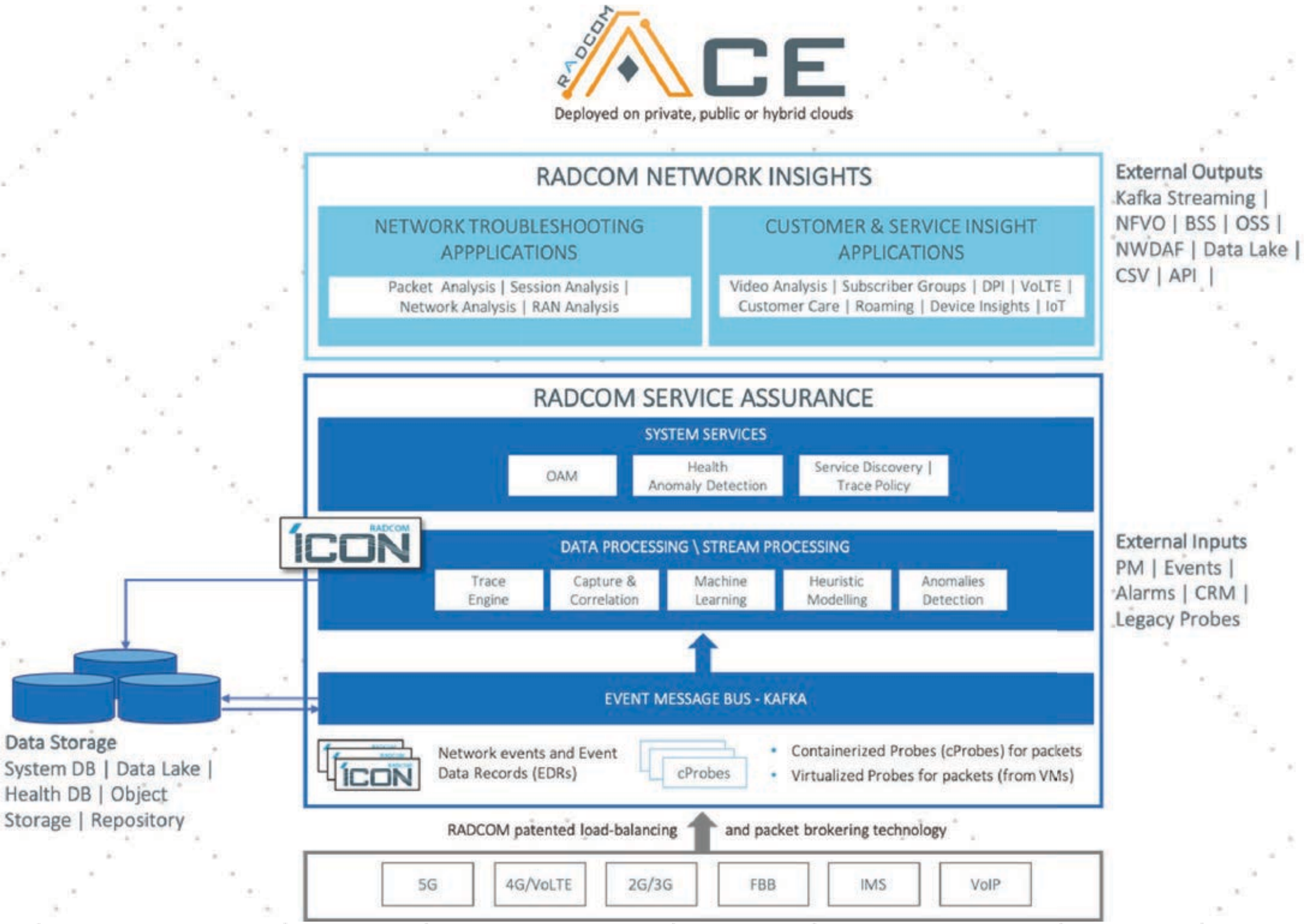
- Tareq Amin, Chief Technology Officer, Rakuten Mobile, Inc.

ABOUT RADCOM

RADCOM (Nasdaq: RDCM) is the leading expert in cloud-native, automated service assurance solutions for telecom operators transitioning to non-standalone and standalone 5G networks.

RADCOM ACE is an automated 5G assurance platform that seamlessly integrates with Kubernetes to provide a closed-loop approach to assurance for Non-Standalone (NSA) and Standalone (SA) 5G.

Being Service Based Architecture (SBA) ready, the solution supports advanced 5G assurance capabilities for end-to-end visibility into the customer experience and service quality for 5G.


RADCOM ACE
Deployed on private, public or hybrid clouds
RADCOM NETWORK INSIGHTS
NETWORK TROUBLESHOOTING APPPLICATIONS
Packet Analysis | Session Analysis | Network Analysis | RAN Analysis
CUSTOMER & SERVICE INSIGHT APPLICATIONS
Video Analysis | Subscriber Groups | DPI | VoLTE | Customer Care | Roaming | Device Insights | IoT
External Outputs
Kafka Streaming | NFVO | BSS | OSS | NWDAF | Data Lake | CSV | API |
RADCOM SERVICE ASSURANCE
SYSTEM SERVICES
OAM
Health Anomaly Detection
Service Discovery | Trace Policy
RADCOM iCON
DATA PROCESSING \ STREAM PROCESSING
Trace Engine
Capture & Correlation
Machine Learning
Heuristic Modelling
Anomalies Detection
External Inputs
PM | Events | Alarms | CRM | Legacy Probes
EVENT MESSAGE BUS - KAFKA
Data Storage
System DB | Data Lake | Health DB | Object Storage | Repository
iCON
Network events and Event Data Records (EDRs)
cProbes
• Containerized Probes (cProbes) for packets
• Virtualized Probes for packets (from VMs)
RADCOM patented load-balancing and packet brokering technology
5G
4G/VoLTE
2G/3G
FBB
IMS
VoIP

ABOUT RADCOM

RADCOM Network Intelligence

The leading solution for 5G, and IoT

RADCOM ACE includes the following containerized solutions: RADCOM Service Assurance, and AI-driven RADCOM Network Insights.

In addition, the solution can work with RADCOM Network Visibility a stand-alone, fully virtualized network packet broker (vNPB) with virtual tapping and filtering.

RADCOM ACE uses streaming analytics to deliver automated real-time network intelligence given to the operators' orchestration to detect, analyze, and resolve issues automatically.

RADCOM ACE also provides end-to-end network troubleshooting from the KPI level down to the session/packet level, critical when rolling out new network architectures.

REFERENCES

[1] TeckNexus, 5G Ecosystem Landscape - Sept 2020 release.

[2] Redhat, Telefónica Movistar Argentina uses cloud to improve customer experience

[3] Redhat, Turkcell creates unified telco cloud with Red Hat OpenStack-based NFV

[4] Ericsson and htpparchive.org, A collaborative approach to encrypted traffic and State of the web

[5] RADCOM, The Case For Automated Assurance In 5G, Aug 2020.

[6] Researchandmarkets, Automation's Rise and the Telecom Engineer, Aug 2020

TeckNexus
DIGITAL SERVICE PROVIDER ECOSYSTEM

5G Research
5G Consulting
5G Tech Talks

5G Ecosystem Hub

- 5G Industry Use Cases
- 5G Vendors
- 5G Solutions

This whitepaper uses publicly available data and figures. TeckNexus has taken all reasonable care and skill in the preparation of this whitepaper. TeckNexus, LLC assumes no responsibility for errors or omissions in the contents of this service & whitepaper publication.

In no event shall TeckNexus, LLC will be liable for any direct, indirect, consequential, special, or incidental damages or any damages whatsoever, whether in an action of contract, negligence, or other arising out of or in connection with the use of this whitepaper.

sales@tecknexus.com
www.tecknexus.com