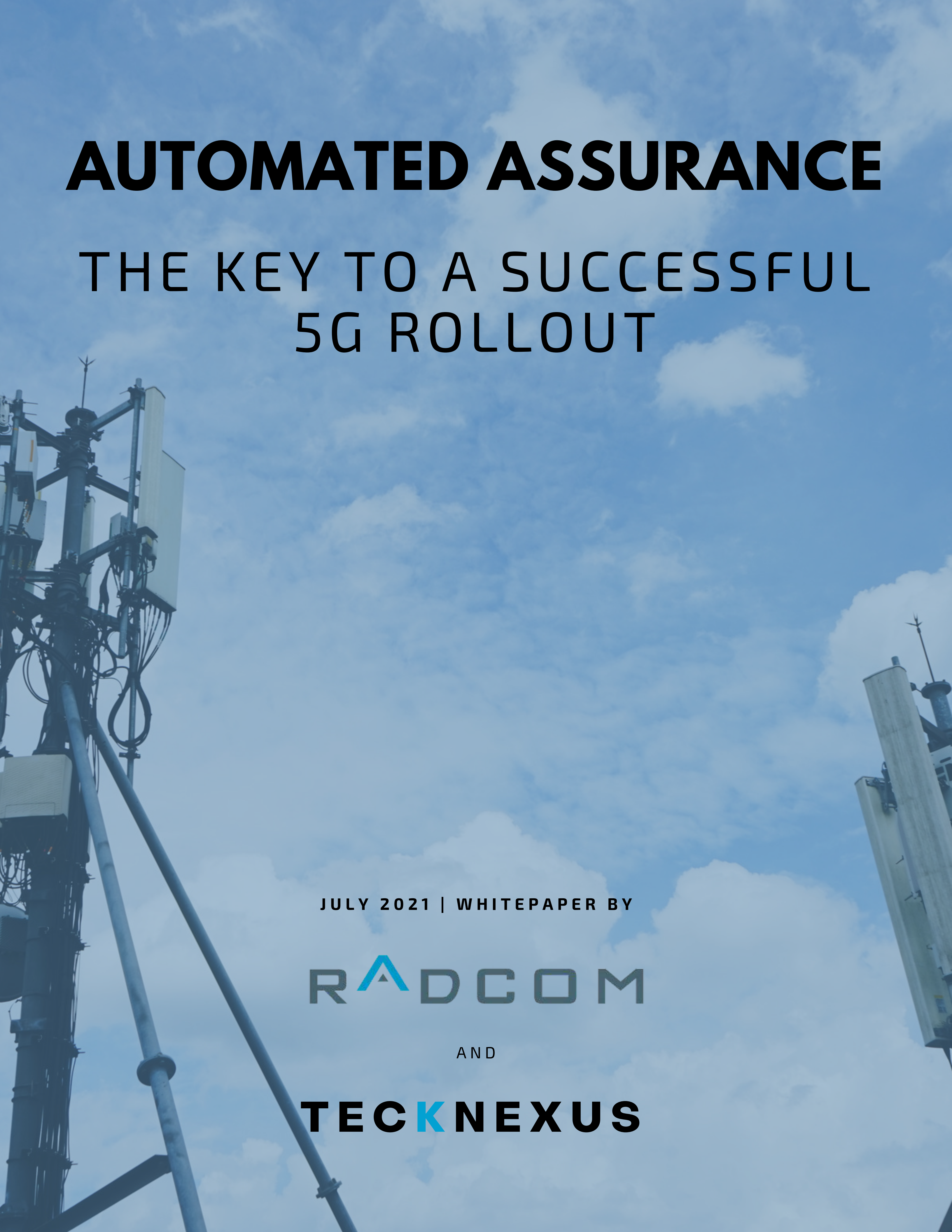

AUTOMATED ASSURANCE

THE KEY TO A SUCCESSFUL 5G ROLLOUT

JULY 2021 | WHITEPAPER BY

RADCOM

AND

TECKNEXUS

TECKNEXUS

BUSINESS CASE FOR AUTOMATED ASSURANCE FOR 5G NETWORKS

Introduction

The business case for:

- Automated 5G assurance
- Predictive Analytics
- End-to-End Monitoring

RADCOM

SOLUTION FOR AUTOMATED ASSURANCE FOR 5G NETWORKS

The solution for:

- Automated 5G assurance
- Predictive Analytics
- End-to-End Monitoring

Reference Operator Assurance Survey, May 2021

MAY 2021

RADCOM

5G ASSURANCE OPERATOR SURVEY

TeckNexus

DIGITAL SERVICE PROVIDER ECOSYSTEM

INTRODUCTION

Global Communications Service Providers (CSPs) are investing heavily in their transition from existing 4G networks to 5G networks.

5G networks bring significantly higher capacity, increased bandwidth, lower latency, ultra-high reliability, and support for a much higher connection density than 4G (a million devices per kilometer square vs. ~2000).

While there are many benefits of the 5G networks, deploying and managing 5G is not easy. 5G networks come with significantly high complexity for:

- Deployment and management of denser networks via a huge number of 5G antennas and Radio Access Network (RAN) hardware components
- Deployment and management of hybrid LTE-NR, i.e., non-standalone 5G, which uses LTE core & access for the New Radio (NR)
- Deployment and management of complex architecture consisting of disaggregated network components from multiple ecosystem vendors, in conjunction with network slicing and edge computing
- Supporting multiple frequency bands, i.e., low, medium, and high spectrum bands
- Scaling the deployment of network resources as needed to ensure network coverage
- Management of the network slices and ensuring related service level agreements with the enterprises
- Real-time visibility into the customer experience across all the services, all the time
- Management of the high volume of traffic, a large number of connected devices, and capturing data from multiple sources
- Integration and management of the public and the private networks

CSPs need to overcome the above complexity and challenges to deliver superior 5G service quality and customer experience. It would also allow them to differentiate their 5G services offering from their competition.

So, how do CSPs overcome the above complexity and challenges for deploying, managing, and assuring the 5G networks? The short answer is automation.

It is becoming apparent to the CSPs that network automation and having real-time end-to-end visibility of their network across all the stages of the 5G network deployment is critical.

As a part of the overall network automation strategy, having an automated, cloud-native assurance solution acting as the independent auditor across all stages of the 5G network, from the lab to full commercial launch providing real-time end-to-end visibility would set the CSPs for a successful rollout of the 5G networks.

This whitepaper focuses on the three critical capabilities that CSPs must have as a part of their assurance solution early on to deliver a superior service quality and customer experience, predictive operations, and highly responsive customer care.

- Automation
- Predictive analytics
- End-to-end monitoring

5G ASSURANCE AUTOMATION

BUSINESS CASE

In 2026, 5G networks will carry more than half of the world's smartphone traffic. The monthly global average usage per smartphone that currently exceeds 10GB is expected to reach 35GB by the end of 2026, as per the *June 2021 Ericsson Mobility report*.

The traditional network monitoring process, which is manual, is ineffective in monitoring this massive volume of increasing data and the complex nature of the 5G networks, as mentioned in the previous section.

CSPs need automation across planning, design, and operations for the network teams as a part of their journey towards closed-loop and zero-touch operations.

~40%

of the responding CSPs think AUTOMATION FOR IMPROVING NETWORK OPERATIONS IS THE TOP PRIORITY FOR NETWORK QUALITY TEAMS

Source: RADCOM and TeckNexus Online Operator Assurance Survey May 2021 | n=100

An automated assurance solution with the below capabilities is essential for CSPs' journey towards zero-touch closed-loop network operations:

- Can be seamlessly deployed on public or private cloud infrastructure, containers, or virtual machines, bare metal, or any combination of these
- Can efficiently scale up/down as needed enabling smooth orchestration and integration with Kubernetes
- Support Service-Based Architecture (SBA) to decipher encrypted traffic by collecting and combining information from multiple sources and multiple event types
- Can efficiently monitor the massive traffic volume and detect anomalies
- Can correlate data collected from multiple sources, including packet feeds, and event-based feeds
- Enables automated root cause analysis and anomaly detection to solve network issues in real-time, thereby proactively improving customer experience

RADCOM SOLUTION

FOR AUTOMATED 5G ASSURANCE

RADCOM ACE is a top-tier cloud-native solution built for automated 5G assurance that seamlessly integrates into the 5G core as a Cloud-Native Function (CNF) and provides real-time subscriber analytics and advanced troubleshooting capabilities.

Built using a microservices architecture, RADCOM ACE allows for efficient scaling and updating. In addition, this Lego-like structure allows for adding and removing microservices and components as needed, keeping it lightweight and agile. Scaling can be controlled automatically based on the load of specific components in the deployment. Scale-up/down is handled without impact on the availability of the system. RADCOM's solution utilizes auto-instantiation, auto-scaling, and re-balancing according to 5G NF service discovery.

RADCOM works with any leading platform and program. With orchestration controlling the containerized functions and enabling network and service assurance automation.

Being cloud-native, the solution integrates with public, private, and hybrid clouds and allows operators to assure the quality of their 5G core services.

Furthermore, it deploys agile software development methodologies using a complete pipeline for CI/CD to rapidly deploy change requests and product customizations, including automatic testing and verification cycles.

This provides a test and measurement solution that quickly evolves with the rapidly changing network environment.

Moreover, the solution utilizes cloud-native probes to manage the high volume of traffic and capture data from multiple sources, ensuring operators gain real-time visibility into the service quality:

- Offers real-time subscriber analytics and troubleshoots network degradations
- Generates XDRs (eXtended Detail Records) per session per subscriber to troubleshoot any issue on the network and identifies its root cause
- Deploys automated assurance containerized and controlled by Kubernetes to integrate and scale as part of the service lifecycle.

PREDICTIVE ANALYTICS

BUSINESS CASE

CSPs face substantial challenges in monitoring and managing the massive amount of 5G data traffic and the complex 5G network architecture.

The success of their 5G rollout depends on whether they can monitor this data efficiently to pinpoint the network degradation issues that directly impact their customers.

The traditional service assurance solutions have been predominately manual and acted in a reactive mode to identify the network faults and remediation of those issues.

The ultra-low latency 5G applications and services requiring high reliability cannot wait for the manual triage and remediation of the network issues. Neither can the network slicing enterprise customers that require guaranteed quality of service.

In short, the significantly time-consuming and resource-intensive traditional assurance approach cannot support monitoring of the complex 5G network.

For detecting and remediation of the 5G network issues, CSPs need an assurance solution that:

- Can create rules and policies that can proactively prevent and resolve the issues
- Can leverage technologies that can analyze massive amounts of data already collected via multiple sources without human intervention
- Predicts the impact of network changes via “what-if” scenarios leveraging advanced Machine Learning (Ml) and Artificial Intelligence (AI) algorithms
- Detects network anomalies and reduces false positives via searching for data that does not match an expected behavior or pattern
- Alerts the Network Operation Center (NOC) engineers of the critical customer-facing issues

~50%

of the responding CSPs think PREDICTIVE ANALYTICS & AUTOMATION HAS THE HIGHEST IMPACT ON THE CUSTOMER EXPERIENCE IN THE 5G NETWORK

Source: RADCOM and TeckNexus Online Operator Assurance Survey May 2021 | n=100

- Automate root-cause analysis and impact analysis based on the number of customers impacted via the AI/ML algorithms
- Takes automated actions to continuously optimize the network, working towards CSP's goal of closed-loop assurance

The sample use cases where CSPs can leverage the predictive analytics assurance capabilities include network performance optimization, network capacity planning, and enhancing customer experience.

RADCOM SOLUTION

FOR PREDICTIVE ANALYTICS

With built-in AI/ML, RADCOM ACE performs KPI-based anomaly detection and predictive insights into the customer experience, allowing operators to receive nearly real-time alerts to a closed-loop approach to network operations.

As a result, it enables operators to assure the customer experience proactively and optimize network performance, improving network uptime by an average of ~10-15%. To do so, RADCOM ACE integrated advanced ML models at its core (such as Prophet for forecasting time series).

When anomalies are detected, either network engineers can be alerted, or automated network actions can be triggered immediately. As anomaly detection relies on ML algorithms that seamlessly correlate data with relevant KPI metrics to provide a complete story for predicting the network's behavior.

These algorithms can identify data patterns over time and across datasets and learn from them. They can also make predictions based on that data to forecast future issues and mimic the human-decision making process by auto-responding to network events.

This will free engineers from monitoring these critical KPIs manually, enabling them to focus on other high-priority issues.

Instead, different departments within the operators' organization, such as the NOC, listen and receive these critical alerts and proactively correct network degradations before subscribers become aware of them.

Having such an assurance solution with built-in AI/ML anomaly detection will enable operators to:

- Analyze the immense amounts of data generated by the network, which no human can do.
- Rapidly identify performance issues across all services.
- Receive alerts if a specific KPI breach occurs.
- Identify patterns over time and group various anomalies to perform automated root-cause analysis in case an issue arises.

Hence, operators can optimize their network most efficiently without the need for manual adaptation, accumulating experience over time to a closed-loop approach for network management.

END-TO-END MONITORING

BUSINESS CASE

5G network architecture includes a new cloud-native 5G Core (5GC) and a new radio access technology (5G NR).

As CSPs transition to the new 5G network technology, they need an automated assurance solution that provides them with real-time end-to-end visibility of their network from RAN to the core.

~50%

of the responding CSPs think END-TO-END (RAN TO CORE) NETWORK MONITORING AND CLOUD-NATIVE SOLUTION ARE THE MOST IMPORTANT FEATURES FOR SELECTING A SERVICE ASSURANCE VENDOR FOR 5G

Source: RADCOM and TeckNexus Online Operator Assurance Survey May 2021 | n=100

RAN MONITORING

It has been estimated that about 70% of all the problems that mobile subscribers experience are due to radio issues.

These radio-related issues, such as lack of coverage or low signal, can result in dropped calls or slow data connections for the customers, resulting in poor customer experience. Hence, already a key concern for the CSPs to monitor the radio access network.

Moreover, with the introduction of the 5G NR, irrespective of whether it uses virtualized RAN or Open RAN technology, it remains the critical network component for delivering 5G services. So, the operators need to monitor RAN effectively.

By monitoring RAN and correlating the monitoring data from 5G Core, the CSPs will be able to determine the root cause of an issue and decide the required remediations.

As CSPs move from low to medium to high-frequency bands, the network performance increases considerably but comes at the cost of the coverage.

Millimeter-wave offers ultra-high bandwidth with Line-of-Sight (LOS) coverage but is susceptible to atmospheric conditions, interference from objects like buildings, and has difficulties penetrating through materials.

Therefore, CSPs have to monitor the quality of customer experience as the throughput can change from gigabits to megabits within few seconds when switching from 5G mmWave cell to standard 5G NR cell.

38%

of the responding CSPs think HANDOVER BETWEEN 4G/5G AND DIFFERENT FREQUENCIES (C-BAND/MILLIMETER-WAVE) ARE THE TOP ASPECTS TO MONITOR

Source: RADCOM and TeckNexus Online Operator Assurance Survey May 2021 | n=100

SLICE MONITORING

One of the potential revenue-generating opportunities for CSPs is network slicing. Network slicing enables CSPs to split the network resources into logical or virtual networks (“slices”) to address specific use cases with distinct characteristics and specific Service Level Agreements (SLA).

A network slice spans across the end-to-end network, i.e., across RAN, edge, transport, and core network.

CSPs can package multiple network slices with different characteristics as a single product targeting customers with specific business needs, e.g., smart cities where CSPs can configure different slices for emergency responders, normal traffic control, and sports avenues.

To assure that the SLAs are met corresponding to each of the network slices within the 5G network, the CSPs must monitor and analyze the traffic corresponding to each of the virtual network slices.

EDGE MONITORING

5G, in combination with edge computing, also referred to as Multi-Access Edge Computing (MEC), enables CSPs to offer new services and business models to consumers and enterprises.

CSPs capitalize their network by opening it to third-party ecosystem players to develop ultra-low latency applications, such as Cloud/VR gaming, AR/VR-based remote training, remote factory monitoring & maintenance.

Since edge computing stores and processes the data close to the origin of the information, CSPs need to extend their monitoring capabilities to cover the network edges.

The assurance solution must proactively detect any network degradations and service impacts at the network edge to ensure that the edge applications deliver on the low-latency requirements.

RADCOM SOLUTION

FOR END-TO-END MONITORING

RADCOM ACE correlates multiple data types (events, EDRs, and network packets) from the 5G NR to the 5G core to ensure a superior customer experience.

It also provides end-to-end network troubleshooting from the KPI level down to the session/packet level, critical when rolling out new 5G network architectures.

RAN MONITORING

RADCOM RAN monitoring lets you gain complete network visibility and understand the root cause of an issue and the correct actions required to resolve it. RAN data includes metrics such as Packet Jitter, Packet Loss, Timeouts, Throughput, and Connection Release Cause that can be collected and measured.

RADCOM ACE fully supports RAN/vRAN/O-RAN and offers real-time subscriber analytics and advanced end-to-end troubleshooting capabilities to ensure a smooth rollout of greenfield RAN technologies and an enhanced user experience.

In addition, RADCOM ACE provides Key Performance Indicators (KPIs), and Key Quality Indicators (KQIs) for 5G RAN running high-band spectrum, enabling you to optimize your mmWave and sub-6 GHz band deployments.

It enables to view and monitor the different parameters for each cell, how they perform, monitor handovers, and help with planning additional cell deployments by mapping out all the devices and where extra coverage is needed.

In addition, RADCOM ACE indicates where there are coverage holes in the current network (for example, by showing that there are many subscribers in certain areas and not receiving the expected 5G service).

For mmWave, a loss of service or drop in quality is vital and much more essential than a standard cell as the effect on the customer experience can be significant.

As these cells continue to be deployed, operators can utilize RADCOM ACE to monitor the quality, coverage, and subscriber usage to optimize their mmWave deployments.

RADCOM's solution helps operators ensure mmWave by continually monitoring:

- Loss of service
- Low throughput
- The control plane (to troubleshoot drops in performance)

Hence, RADCOM ACE provides you with end-to-end visibility into greenfield RAN technology (running low, mid, and high-band spectrum). Enabling you to seamlessly integrate mmWave into your network, optimize 5G RAN performance, and provide a consistent, high-quality customer experience.

SLICE MONITORING

RADCOM ACE continuously monitors each virtual slice, mapping every XDR/KPI/KQI to the relevant service slice to understand the overall QoE and QoS and confirming compliance to SLAs.

If SLAs aren't being met, alerts and alarms can be set to notify if anomalies are detected and if any service level requirements are breached.

Engineers can use KPI/KQI dashboards to monitor their slices and drill down from a macro to a micro view using tracing tools to perform an in-depth analysis of the network slice performance and perform root cause analysis of any degradations in service.

Capabilities include:

- Visibility into your network slices and their QoS/QoE
- Advanced troubleshooting and root cause analysis to find and resolve issues quickly
- Proactive and continuous monitoring of QoE and QoS to confirm SLAs.

EDGE MONITORING

To exploit the full power of edge computing, operators' service offering at the edge needs to meet stringent SLAs of business-specific use cases and applications.

To do so, you must be able to detect network degradations and prevent service outages proactively. Thus, monitoring each edge-delivered service smartly, meeting agreed-upon SLAs – making assurance a critical success factor.

To achieve that, operators should deploy a distributed assurance solution to gain visibility into services at the edge to optimize the network performance and deliver the expected quality.

RADCOM ACE is a distributed assurance solution that is microservices-based can deploy micro-probes with a low footprint that are scalable at the edge.

In addition, the micro-probes will be instantiated with the network function to provide troubleshooting capabilities and deliver real-time intelligence so operators can proactively ensure new low-latency service offerings.

RADCOM

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

RADCOM provides a suite of fully containerized 5G solutions that enable operators to smartly monitor and optimize 5G from the RAN to the core, including network slicing and edge computing. By correlating multiple data sources (network events, event data records, and network packets) our solutions provide smart, AI-driven insights, to ensure a superior 5G customer experience.

To learn more about our 5G assurance solution click here.

TECKNEXUS

5G MAGAZINES | 5G RESEARCH | 5G CONSULTING | 5G ECOSYSTEM HUB

www.tecknexus.com

contact@tecknexus.com

TeckNexus has taken all reasonable care and skill in the preparation of this document. TeckNexus, LLC assumes no responsibility for errors or omissions in the contents of this service & document 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 document.