PRODUCED BY

LightReading

SPONSORED BY

NETSCOUT®

5G SIGNALS NEW CHALLENGES WITH NETWORK MONITORING & PERFORMANCE

CONTENT

03
Authors

04
Introduction

05
5G's future includes a cloud-native architecture complete with containers

07
Verizon tests new 5G security tech

09
Q&A with Dr. Vikram Saksena

12
5G transport: Putting networks to the test

14
Toward cloud-native 5G core

16
5G makes virtualization vital, not optional

20
Resources

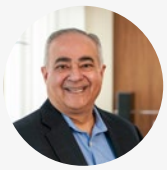
ABOUT THE AUTHORS & CONTRIBUTORS

Karen Brown
Industry Writer
Light Reading

Karen Brown is an industry writer and analyst with an extensive background cable, telco and wireless providers as well as associated technology providers. Her resume includes stints as a reporter at Cable World Magazine, Multichannel News, Wireless Week and CED, and as an analyst at One Touch Communications.

Sue Marek
Special Contributor
Light Reading

Sue Marek has been reporting on the telecom and tech industries for more than 25 years. Most recently she was editor in chief at SDxCentral where she oversaw all of that site's editorial content. Prior to that she was editor in chief of FierceMarkets Telecom Group, where she managed a team of editors and was responsible for the content for several of the company's web sites, newsletters and live events. Sue is a frequent speaker at industry events and has moderated panels for the Consumer Electronics Show, the Competitive Carriers' Show, The Wireless Infrastructure Show, 5G North America, DC 5G, Interop, and more.



Dr. Vikram Saksena
Chief Solutions Architect
NETSCOUT

As chief solutions architect for NETSCOUT, Vikram Saksena is customer-focused, working closely with the company's sales team to identify and drive revenue opportunities in fixed and wireless networks, data center transformations, cloud visibility and monitoring, application and network peformance management, and unified communications and collaboration.

Saksena is a subject matter expert in modern-day technologies, such as 5G automation, fixed and mobile broadband, cloud computing, network and data center virtualization, Internet of Things (IoT), and software-defined networks and analytics.

He is a former Massachusetts Technology Leadership Council "CTO of the Year" finalist and a distinguished alumni at the University of Illinois, where he holds a Ph.D. in electrical engineering. He was honored as a gold medalist at the Indian Institute of Technology, where he is also a distinguished alumni. Saksena currently represents NETSCOUT on the board of the Alliance for Telecommunications Industry Solutions (ATIS) and Linux Foundation's Open Networking Alliance.

Gabriel Brown
Principal Analyst – Mobile Networks & 5G
Heavy Reading

Gabriel covers the mobile network system architecture, including evolution of the RAN, the mobile core, and service-layer platforms and applications. Key technologies in his coverage area include LTE Advanced, small cells, Evolved Packet Core, carrier WiFi, and software-centric networking technologies such as NFV, SDN, and service chaining. Gabriel has covered mobile networking since 1998 through published research, live events, operator surveys, and custom consulting. Prior to joining Heavy Reading, Gabriel was Chief Analyst for Light Reading Insider research service; before that, he was editor of IP Wireline and Wireless Week at London's Euromoney Institutional Investor. He is based in London.

Sterling Perrin
Senior Principal Analyst –
Optical Networking & Transport
Heavy Reading

Sterling has more than 15 years' experience in telecommunications as an industry analyst and journalist. His coverage area at Heavy Reading is optical networking, including packet-optical transport. He also authors Heavy Reading's Packet-Enabled Optical Networking Market Tracker and Next-Gen Core Packet-Optical Market Tracker. Sterling joined Heavy Reading after five years at IDC, where he served as lead optical networks analyst, responsible for the firm's optical networking subscription research and custom consulting activities.

Bruce Kelley
Chief Technology Officer
NETSCOUT

As Senior Vice President and Chief Technology Officer for NETSCOUT, Bruce Kelley works closely with every facet of the organization, interfacing with all departments from sales to product management to engineering. He plays a lead role in setting the priorities and direction around product and service developments in the service provider business. Highly regarded in the technology space as a 5G, IoT, edge cloud and automation visionary and expert, Bruce regularly consults with service providers to identify challenges related to network monitoring in order to achieve service and security assurance. He is a staunch advocate of the importance of delivering end-to-end visibility across today's increasingly complex data center architectures. Bruce uses knowledge gleaned over decades to guide how current and next-generation technologies will impact operations and delivery of services across the service provider space. He is the holder of more than 40 patents for technology-related innovations.

INTRODUCTION

5G SIGNALS NEW CHALLENGES WITH NETWORK MONITORING AND PERFORMANCE

As with other groundbreaking new technologies, 5G presents a double-edged sword. While it supports an array of attractive, cutting-edge applications for enterprises and consumers, it also requires a sharper focus on network control, management and security issues.

Indeed, assuring network monitoring and control becomes more critical as the industry transitions from the initial non-standalone 5G framework that relied on a 4G network core to a fully 5G standalone scheme. The non-standalone scheme helped to speed adoption of 5G, but the standalone upgrade provides the real payoff for operators, offering edge compute and cloud native capabilities.

This lays the groundwork for consumer applications such as low-latency artificial reality/virtual reality (AR/VR) video and cloud gaming, and it supports new and potentially lucrative enterprise applications with faster response times thanks to 5G standalone's network edge elements. 5G's ability to blend a wider range of wireless spectrum including cellular, unlicensed and licensed mid-band and millimeter wave (mm Wave) frequencies also gives operators new opportunities to deliver more flexible hybrid fixed and mobile services with expanded reach and data speeds.

But with these rewards come risks. Standalone 5G is more complex, and the more complex a thing is, the easier it is to break. So 5G carriers face greater threat of network disruption from software update bugs, competition for resources among network elements and cyberattacks launched by bad actors.

In response, 5G operators are turning to network automation and Open Radio Access Network (RAN) platforms to improve network control and monitoring. That includes Industry 4.0, a platform developed for the manufacturing sector that provides automated management and 5G wireless connectivity for robotic Internet of Things (IoT) devices, all with analytics to monitor and flag quality control issues.

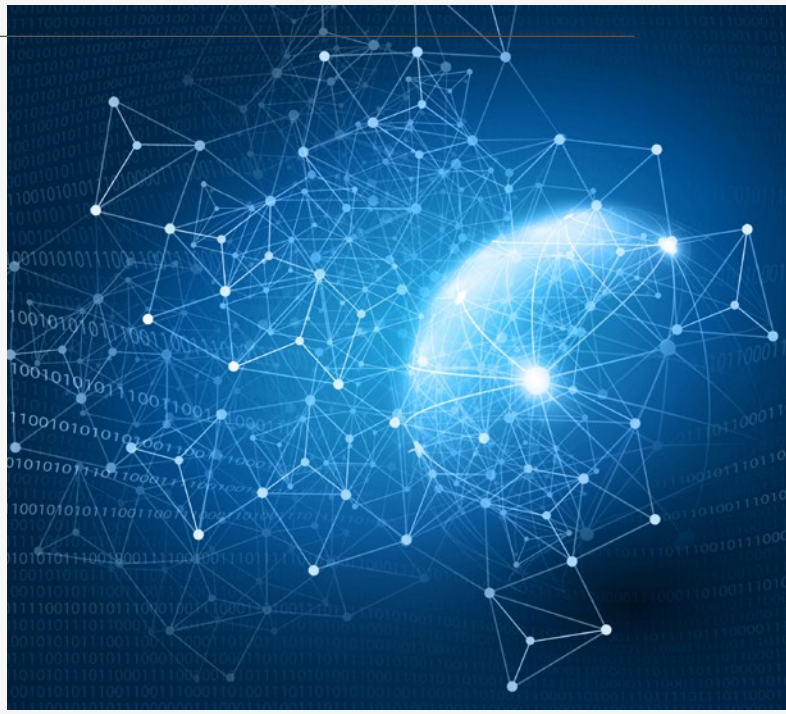
Open RAN, meanwhile, offers potential advantages in 5G buildout and operations. Unlike traditional 2G/3G/4G wireless architectures that rely on proprietary hardware and software, Open RAN is based on open standards, allowing operators to mix and match network elements from multiple vendors. The result can be lower cost, increased interoperability and better visibility across 5G network deployments.

Given these issues, there is a lot at stake for 5G wireless operators. This report delves into issues presented by fast-evolving 5G technology, and how wireless network operators can minimize their risks while maximizing their rewards in the coming years.

Karen Brown
Industry Writer
Light Reading

5G'S FUTURE INCLUDES A CLOUD-NATIVE ARCHITECTURE COMPLETE WITH CONTAINERS

When it comes to standalone 5G networks, many of the world's largest mobile operators are considering moving to a cloud-native network architecture coupled with containers.



A container is a standard unit of software that combines code and all of its dependencies into one package. The benefits of using containers are that they allow applications to be deployed quickly, efficiently and securely.

Inspired by the openness of the IT industry, many mobile operators believe that a cloud-native architecture coupled with containers will help them develop and deploy telecom networks more quickly and make it possible for them to respond to the explosion in mobile data traffic and the growth in wireless connections.

According to Marisa Viveros, vice president of strategy and offerings, telecommunications, media and entertainment at IBM, containers are key to deploying 5G because a 5G network will deliver ultra-high speeds and low latency. "If you are going to have these super-fast networks you want applications to be equally fast. You want the applications moving and you want workloads to be placed where it makes the most sense," she said, noting that containers will make that possible.

Rakuten's Chief Technology Officer Tareq Amin recently said that the mobile operator's existing architecture is not exactly what he wants because it's still using virtual machines (VMs). His vision is to have a network based on lightweight containers that will break functions down into smaller, configurable components. Rakuten's long-term plan is to have a container-based platform that resides on Rakuten's own cloud.

Amin's statement was unique because wireless operators usually aren't very vocal about their use of containers. Viveros said that telcos don't usually talk about containers when they discuss their network because they focus more on the applications. But she added that operators are definitely aware of the advantages of containers. "Containers have less overhead and require less payloads on the system resources than virtualized machines," she said. Plus, they also provide more portability. "Applications can be running in various containers and you don't have to worry about the operating system or the hardware."

Rakuten isn't alone in its container aspirations. In July 2019, Verizon announced it was working on a proof-of-concept trial in a live network of a container-based wireless evolved packet core. According to Folke Anger, solution line head for packet core at Ericsson, it was important for the vendor to work with an operator that was technically very advanced and had a lot of demands on the network. "We moved some of the evolved packet core applications into a container," Anger said.

Anger added that other operators are also starting to move core network functions into cloud-native network functions. "If you have cloud-native, you need containers."

Verizon talked about its move to a cloud-native network at the recent Red Hat Summit 2020 virtual conference. Srini Kalapala, vice president of technology and supplier strategy at Verizon, said that Verizon is working to bring a truly cloud-native stack to its 5G network. "We are working with you [Red Hat] to bring that capability to our networks. From the RAN to the core it will be built on a cloud-native stack," Kalapala said.

Kalapala added that Verizon has been on this evolutionary path since 2015 and 2016 when it first started virtualizing its network and separating the hardware from the software. "Telcos are following the webscale companies and we are a little behind," he said.

ONAP's Frankfurt release

The Linux Foundation's Open Networking Automation Platform (ONAP) just issued its sixth release, called Frankfurt, which includes a blueprint for operators to scale their 5G networks and includes cloud-native network functions and containerized functions.

ONAP is an open-source software platform that was formed in 2017 after the Linux Foundation combined AT&T's E-COMP platform with OPEN-O, which was a group founded by China Mobile.

The Frankfurt release also introduces end-to-end network slicing with modeling and orchestration of a network slice, including 5G RAN, core and transport network slice elements.

According to the Linux Foundation's Arpit Joshipura, general manager of networking, edge and IoT, the 5G network is a hybrid where VMs will reside with containerized network functions (CNFs). "Containers and VMs have to work together," he said.

Along with the release of Frankfurt, the Linux Foundation also provided details of different operator case studies that involve a cloud-native network architecture. Operators including China Mobile, AT&T, Verizon, Orange and others are in various stages of implementing Frankfurt but have different strategies and different types of deployments.

VMs and containers

Despite the fact that many operators are interested in containers, Viveros said that she believes most operators will have a combination of VMs, containers and physical hardware in their networks. "I think that telcos are going to run networks in the future that use both VMs and containers. They can't decommission what they already have because it will be too expensive," she added. "And some will continue to run the physical network, the virtualized network and the containerized network. They can mix and match depending upon the topology and geographic locations."

That sentiment was echoed by Ericsson's Anger. "There will be a combination of physical, VNFs [virtual network functions], and the cloud native [architecture]."

But Anger also added that although most operators are looking to containers for their 5G deployments, they can be used in a 4G environment. "We have 4G network functions in the evolved packet core."

In addition, Anger said it is possible to have a cloud-native dual-mode network that supports LTE and 5G non-standalone and the 5G core. Anger said that this capability is important for operators that are still seeing a lot of growth in their 4G LTE network.

Although mobile operators may be in the early stages of working with containers, this technology is viewed as being a key component for making 5G networks agile and efficient.

Sue Marek
Special Contributor
Light Reading.

VERIZON TESTS NEW 5G SECURITY TECH

NEW YORK – Verizon's Network Security engineers recently engaged in a series of successful trials to future-proof its 5G network against security threats and advance security measures to protect the confidentiality, integrity and availability of Verizon's 5G network.

The advent of 5G wireless communications constitutes a new era of network connectivity that will revolutionize many aspects of commerce and our personal lives. Along with new technology comes the need for new security measures. Verizon is focused on protecting against threats to customers' security and ensuring the reliability and resilience of communications services against all manner of hazards, including cyber threats.

"As the design and deployment of networks becomes more complicated and the capabilities of networks allow for much more robust systems, securing those networks is the highest priority," said Srini Kalapala, Vice President of Network Planning for Verizon. "Not only has our network team built our 5G network with industry-leading security, but our team is anticipating and planning for future security issues to protect our network and mitigate risks today and in the future."

Advancing the future of 5G security

While Verizon boasts a highly secure 5G network presently, Verizon engineers are continuing to drive innovation and leadership in the area of cyber security, knowing that threats evolve nearly as quickly as new technology is introduced. To that end, Verizon engineers and partners are advancing the following initiatives:

1. **Security Network Accelerators to improve latency and operational efficiency**
   As network operations become more complex, additional purpose-built hardware supporting security functions such as firewalls, IDS, DDoS, Probes and Packet brokers are deployed throughout the network. The addition of this hardware introduces additional latency and opens the door for greater maintenance as well as additional points of vulnerability. To solve for this, Verizon engineers have virtualized many of these functions and moved them to the cloud. However, for higher performance security functions, Verizon engineers are working to install programmable network accelerators as a way to mesh together multiple high performance, latency dependent security functions into a single, AI ML driven Network Accelerator, reducing operational expenses, reducing reliance on programming by people and increasing the efficiency of delivering these security functions. Verizon is working with the University of California Santa Barbara to develop AI ML driven firewall and IDS capabilities that are able to be delivered in a whitebox network accelerator.

2. **AI/ML Security**
   AI/ML is a technology that is being broadly adopted in all industries, including 5G, to automate decision making, troubleshooting, forecasting, network management, security, and more. With the acceleration in use of AI ML throughout networks, Verizon engineers are developing an AI ML Security Framework which will offer additional protection in the AI ML models that power the network. This AI ML Security Framework will help verify the providence of information being fed into AI ML algorithms, ensure the AI ML models are operating correctly, and will manage the security around where that information goes and how it is interpreted and used. Verizon engineers are trialing the framework in two AI ML use cases at present; one to detect security anomalies in the network and the other to analyze MIMO antenna performance at cell tower.

3. **Machine State Integrity (MSI)**
   Understanding the criticality of both the confidentiality and integrity of data, Verizon is working with Guardtime and WWT to provide near real-time, non-repudiated evidence of tampering in a machine's state while also providing meaningful reductions in time between a machine's compromise and its detection. If a security breech or incident occurs, it is critical to be able to quickly identify changes in data. With the amount of data stored in systems today, identifying breeches in data integrity can be a time consuming and onerous task. Verizon engineers and our vendors are using cryptographically secure functions to create digital fingerprints of data and store them in a blockchain so they cannot be modified. These fingerprints are fully secure, unhackable and accessible anywhere in the world. By comparing fingerprints stored in the blockchain to fingerprints taken during or after a cyber attack, companies can more quickly and easily determine if the integrity of their data was compromised. Verizon, Guardtime and WWT are preparing for trials of this new technology to begin. When complete, Verizon engineers will be able to leverage machine state integrity to more effectively protect the data on the Verizon network including configuration of towers, Verizon Cloud servers and more.

4. **Secure Credentialing Management System (SCMS) for Connected Vehicles**
   Connected vehicles need to connect to each other, to roadside infrastructure, to other road users and to cloud-based services. SCMS is the fundamental mechanism to ensure those connections are protected against attacks on integrity, confidentiality, and repudiation. The SCMS provides digitally signed certificates and activation codes that are used to validate vehicle safety messages. For the first time in the Connected Vehicle industry, a joint Verizon and LG team effort validated and secured CV2X Basic Safety Messages (BSMs) using a standards-compliant SCMS hosted on a Verizon 5G MEC. This milestone was completed at the Mcity Test Track in Ann Arbor, MI and validates Verizon's core capabilities in 5G network connectivity. It also demonstrates how 5G MEC can be leveraged for public safety and Connected Vehicle security.

Security of Verizon's 5G Network

In addition to advancing future security initiatives, Verizon's Network Security team recently produced a white paper entitled "The Security of Verizon's 5G Network" which describes how every element of Verizon's 5G network implements security controls that deliver confidentiality, integrity, and availability so the overall network provides subscribers with a secure communications channel. The paper highlights security initiatives including:

- Leveraging Verizon's global security capabilities
- Deploying security features from 5G standards
- Enhancing security via features specific to Verizon's 5G implementation
- Enabling customer-facing security services

"In all aspects of our network, from the core of the network, to the radio access edge, even to the customer device, we have built our network to be secure," said Kalapala. "From design, to implementation, to deployment the 5G network, built on the foundation of the best 4G security, is the gold-standard in the industry. We will not compromise when it comes to the security of our network and that of our customers' data."

This new white paper comes on the heels of an additional security white paper which describes how the new architecture and capabilities of 5G networks will allow operators to detect and address cyber threats faster and more efficiently than ever before.

Verizon

SPONSOR CONTENT

Q&A WITH DR. VIKRAM SAKSENA

CHIEF SOLUTIONS ARCHITECT
NETSCOUT

Light Reading asked Dr. Vikram Saksena of NETSCOUT'S CTO office to share insights into how 5G will transform business, and why 5G is such a game changer for both service providers and enterprises. He shared the challenges customers face and how NETSCOUT'S Visibility Without Borders is helping customers meet the end-through-end visibility challenges required to succeed in this exciting market.

5G is such a hot industry topic. What is the state of 5G deployments today, and what is NETSCOUT's experience in those deployments?

The state of 5G in all global markets started within a non-standalone framework, where 5G radios were deployed with a 4G core network. I see this initial deployment as a benchmark for testing the market to ensure that the 5G radio access network (RAN) was delivering the expected performance.

However, as 5G evolves, customers are slowly transitioning to standalone 5G. Its edge computing capabilities and distributed cloud-native core are where the real power of 5G comes into play. Moving forward with standalone deployments, NETSCOUT can really help customers succeed because our suite of technologies provide end-through-end monitoring across the edge, core and into the control plane and user plane.

NETSCOUT continues to monitor the non-standalone network from its incumbent position in the 4G core. The new area of focus has been to help our customers with RAN planning using our unique set of propagation modeling tools. With mm Wave frequencies, this is a very challenging problem for carriers. They need to ensure optimized base station coverage while minimizing the cost of RAN.

With RAN planning on the top of carriers' minds, how disruptive is open RAN technology in the 5G ecosystem and why is it vital?

Open RAN is very important because RAN is the last closed and proprietary element of the wireless network. The opening up of the RAN is the final step to ensure that the entire wireless network is built with open technologies. The network needs to support industry standard platforms and Application Programming Interfaces (APIs) for enabling new programmable capabilities. An open architecture from the RAN to the core will enable rapid service innovation and allow carriers to quickly monetize their investments.

Open RAN also simplifies operations for carriers because it removes dependence and lock-in to proprietary platforms. Open RAN allows carriers to lower capex and opex, and to source technology from best-of-breed industry leaders. This allows seamless management of the RAN and core in an integrated manner. Open RAN, as it becomes integrated with 5G networks, will provide a powerful platform for next-generation applications.

Q&A WITH DR. VIKRAM, CONTINUED

Why is 5G such a game changer? And what are enterprises looking for in the future with 5G and this powerful platform?

5G is a game changer because it brings together wireless technology and cloud computing in a way that has never been done before. As we all know, cloud computing plays a key role in enterprise IT infrastructures due to its flexibility in supporting agile service deployments.

5G also allows carriers to integrate cloud technology within their wireless access infrastructure to bring service agility to the edge. This capability enables enterprises to host low-latency applications at the carrier edge, making it possible to deploy a new generation of applications for digital transformation that were not possible until now. These capabilities serve new and exciting consumer applications like cloud gaming and AR/VR, as well as low-latency Industry 4.0 applications for enterprises at the edge.

How is the enterprise market going to take advantage of Industry 4.0 with 5G?

Industry 4.0 will allow manufacturing companies to automate their process models while introducing smart sensors, robotics and artificial intelligence with data analytics to drive out process inefficiencies.

These technologies will play a critical role in 5G because of their low-latency requirements.

We will see factory automation leading the way with other industries following, such as healthcare, transportation and energy. Even though there aren't any significant deployments yet for enterprises with this process model, we do see some recent pockets of deployments around the globe. For the consumer segment, the demand for 5G is currently muted as we wait for more 5G-ready devices including cloud gaming and other augmented reality applications to come to market.

With edge making a lot of this possible, what is the main challenge in assuring these services at the edge? What is the role of the edge in supporting Industry 4.0 applications in a 5G network?

Clearly, edge computing plays a key role in enterprise services and particularly in Industry 4.0. The edge is required to support low-latency applications – autonomous vehicles, robots and healthcare. These applications will not work effectively without the edge. The challenge is that when services are delivered from the core of the network, the latency requirements are much higher than these applications can tolerate.

Q&A WITH DR. VIKRAM, CONTINUED

Many carriers are building out the edge using some form of cloud native technology, either with private cloud platforms or partnering with public cloud vendors. A cloud-native edge environment yields the best response for 5G because of agility, flexibility and its ability to support low latency as required by next-generation applications.

With this great innovation at the edge, we know there is risk involved. What are the security challenges and required approaches with 5G? How do you mitigate this risk in a wireless network?

Enterprise applications and Industry 4.0 will elevate the need for security for mission-critical and business-critical applications. These critical services must be completely secured to prevent loss of life, loss of business or network failure through compromised devices.

Challenges known in traditional Internet – hacker and bot attacks – must be approached in a new way. Traditionally, traffic is dropped from the network when a compromise is detected; this won't work in the wireless network environment due to user and control plane interactions. A new approach is required to determine how to adapt current Distributed Denial of Service (DDoS) tools to mitigate security challenges within a wireless network.

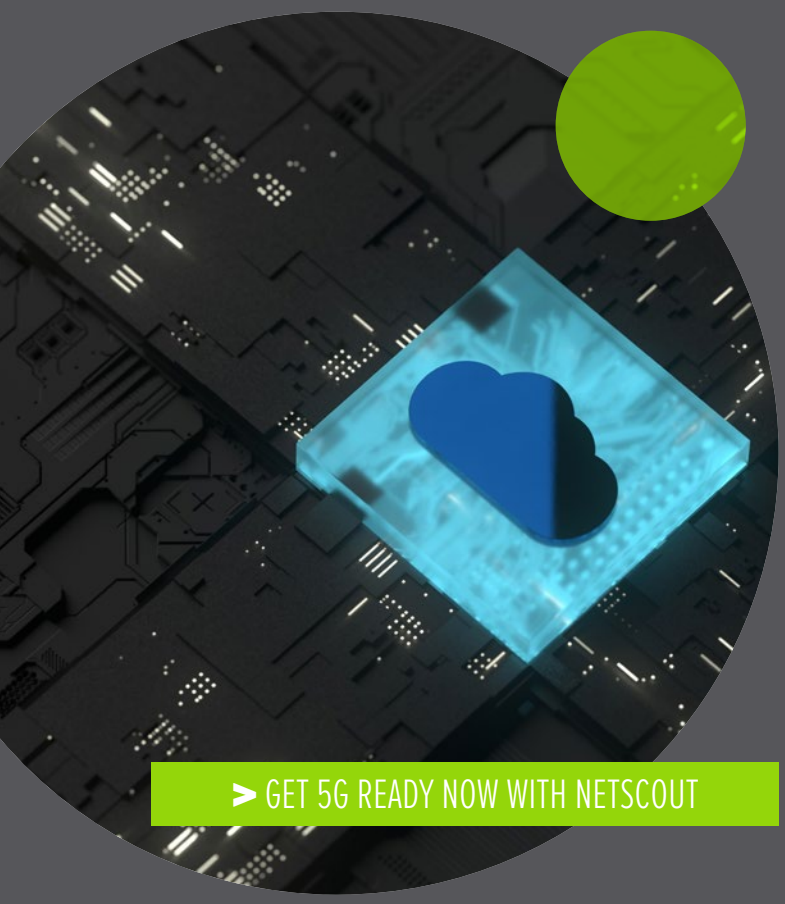
Dr. Vikram, thank you for sharing your insight. How is NETSCOUT meeting current and future 5G industry needs? What is NETSCOUT's unique advantage in assisting customers?

Our solutions have tremendous depth and breadth and provide end-through-end service and security assurance. We call this Visibility Without Borders, which means our solution can cross fixed and wireless network technology boundaries to deliver assurance in any environment – enterprise, consumer, or private 5G.

NETSCOUT's cloud-native solution scales from a very low footprint required for the user plane at the edge to high volumes of traffic in the core for control plane, user plane, and application layer. Our cloud-based service assurance technology can scale in any edge compute environment to monitor performance, assure availability, and ensure security of user plane applications and services. And with open RAN, NETSCOUT can directly assure services from the edge – deploying its scalable cloud-native technology for monitoring while using standard API functions to provide application assurance.

NETSCOUT brings great value to the enterprise customer landscape. Our end-through-end solutions provide monitoring for all mission-critical and business-critical 5G application and services.

5G will continue to transform businesses, and we are in a unique position to assist our customers now and to support future deployments. We're excited about the business opportunities that 5G will bring for both our enterprise and service provider customers.



> GET 5G READY NOW WITH NETSCOUT

5G TRANSPORT: PUTTING NETWORKS TO THE TEST

As 2020 marches on, it is clear that 5G is not sitting still. The long-awaited 3GPP Release 16 freeze occurred in July, just a couple months off schedule due to COVID-19. With limited delays caused by the pandemic, the 5G commercial launch schedule continues largely as predicted. Omdia's latest forecast, published in June, projects that the top 20 global markets will reach 231 million 5G subscribers by year-end – a 15x increase over 2019.

In order to understand how transport networks will evolve to support 5G services, Heavy Reading launched the Operator Strategies for 5G Transport Market Leadership Study with collaboration partners Anritsu, Ericsson, Fujitsu and Infinera in May 2020. The survey attracted 86 qualified network operator respondents from around the world that shared their views on transport deployment issues and timelines, fronthaul networks and radio access network (RAN) centralization, routing and synchronization, and testing 5G networks.

This blog, the third in a four-part series highlighting the key findings from the 2020 study, focuses on testing implications for 5G networks.

Interoperability in an open RAN

One of the fundamental differentiators and benefits of 5G architectures compared to previous mobile generations is the decomposition of the RAN into functional components. These include antenna units (AUs), radio units (RUs), distributed units (DUs) and centralized units (CUs) with the corresponding connectivity segments of fronthaul (RU to DU), midhaul (DU to CU) and backhaul (CU to mobile core). One operator benefit is that greater flexibility drives greater coordination and efficiencies in the RAN. Another benefit is the prospect of an open RAN comprised of functional components supplied by different radio vendors — including new entrants.

Looking at the trend in opening the RAN, Heavy Reading wanted to better understand how operators seek to ensure interoperability among the various RAN components. Specifically, the survey asked: "For your organization, what are the most important testing methods to ensure interoperability in an open RAN environment, such as defined by the O-RAN Alliance and Telecom Infra Project (TIP)?"

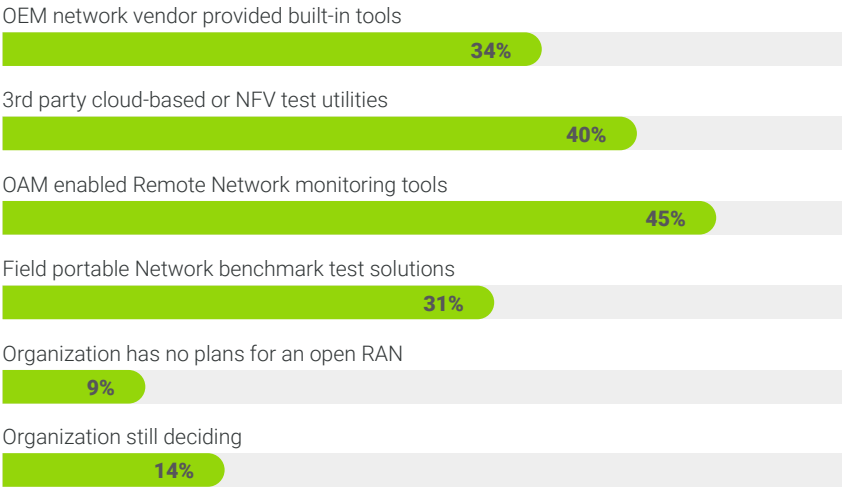
In the rankings, two methods rose to the top. Operations, administration and maintenance (OA&M)-enabled remote network monitoring tools ranked first (selected by 45% of respondents) and was followed by third-party cloud-based or network functions virtualization (NFV) test utilities (selected by 40%). The remote and cloud-based testing ranked above both vendor equipment built-in tools (selected by 34%) and field portable tools (selected by 31%). Results indicate that operators want remote testing abilities when possible.

Measuring fronthaul performance

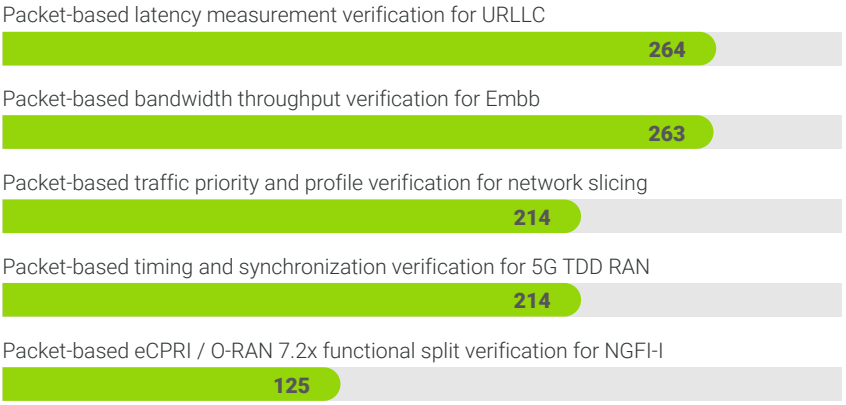
As noted in previous analysis, the centralization of the RAN and the creation of the new fronthaul transport segment pose particular challenges for operators. These are due to greater bandwidth requirements combined with stringent performance requirements relative to other transport segments.

The fronthaul networks pose challenges for operators from a testing perspective, as well. Heavy Reading asked operators to rank next-generation fronthaul performance requirements on a scale of 1 to 5, with 1 being the most challenging and 5 being the least challenging. Weighted scores were generated based on assigned priority.

Most important testing methods in open RAN environments
n=85 (Source: Heavy Reading)



Most challenging performance requirements for next-gen fronthaul networks
n=76 (Source: Heavy Reading)



Note: The score is calculated by assigning a weight to each rating where the highest priority rating holds the highest weight.

With weighted scores of 264 and 263, respectively, packet-based latency measurement verification for ultra-reliable low latency communications (URLLC) applications and packet-based bandwidth throughput verification for enhanced mobile broadband (eMBB) applications were essentially tied at the top of the performance requirement challenges list. Tied for third (with equal weighted scored of 214) were packet-based traffic priority and profiled verification for network slicing and packet-based timing/synchronization verification for 5G. At a distant fifth position, and the least challenging, was packet-based eCPRI/O-RAN 7.2x functional split verification.

Sterling Perrin
Senior Principal Analyst – Optical Networking & Transport
Heavy Reading

TOWARD CLOUD-NATIVE 5G CORE

There are many good reasons for operators to deploy a new core network and move to 5G standalone (SA). But offering services linked to new 5G capabilities such as network slicing, edge applications, fixed/mobile convergence and — in time — ultra-reliable low-latency communications (URLLC) is the primary motivation.

However, the transition to 5G SA is also an opportunity for operators to introduce a new operating model that is agile and efficient. By modernizing their core network infrastructure, operators can achieve greater automation, new scaling and resiliency models, and new methods of network and service orchestration. Clearly, advanced services and advanced infrastructure go hand-in-hand.

So how should operators introduce 5G core (5GC) from a network infrastructure perspective?

The 3GPP Service-Based Architecture (SBA) for 5GC specifies a functional architecture and standardized interfaces. And although implementation is the choice of the operator or vendor, in practice, the expectation is that 5GC will be deployed on software-defined infrastructure. It is increasingly clear that this means a "cloud-native" deployment. In broad terms, this means 5GC implementations that use microservices, containers, centralized orchestration, CI/CD, open APIs, service meshes, and so on.

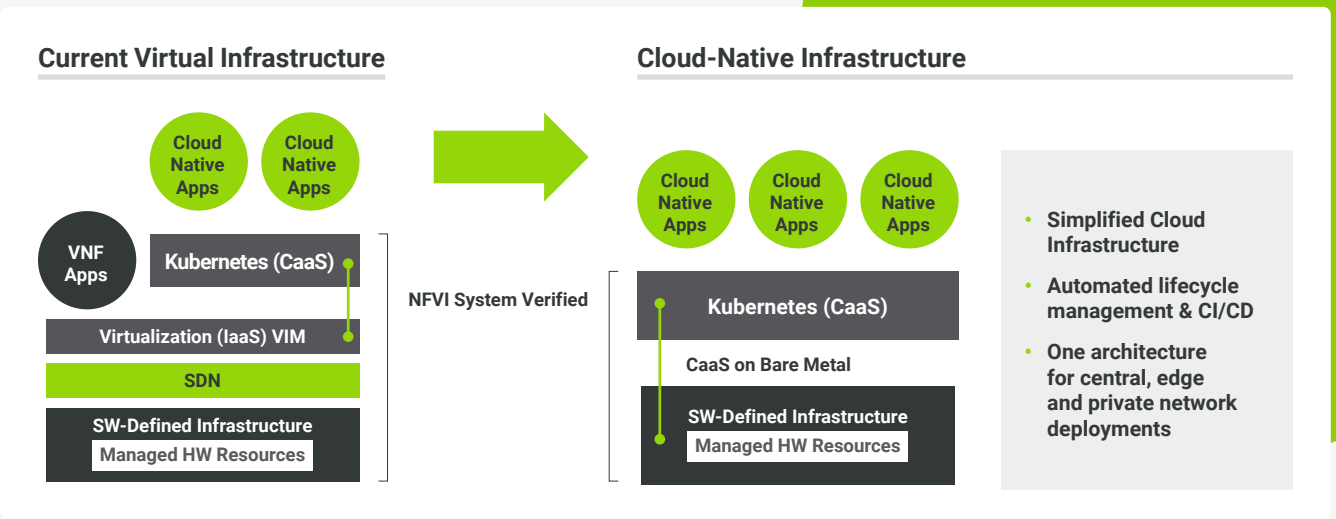
But while the target for 5GC is clear enough, how to make the transition? And what role should operators' existing virtual infrastructure play? The answer to these questions depends on careful calibration of factors such as the commercial launch timeline, the stability of the operator's infrastructure platform, the maturity of the operations team, network vendor product readiness and the penetration of SA-compatible devices in the customer base.

Interim virtual infrastructure platforms to support 5GC...

The following figure shows how today's virtual infrastructure platforms, originally designed for network functions virtualization (NFV), can be used to support 5GC ahead of a transition to cloud-native infrastructure.

Cloud-native 5G core infrastructure

(Source: Ericsson)



To the left, the figure shows the NFV infrastructure stack that, in most advanced operators, is now a mature platform with well-tested operating models and a high degree of availability/reliability. This can run both virtual network function (VNF) and cloud-native apps that make up 4G and 5GC networks. In this scenario, VNFs run, as expected, in virtual machines (VMs). Cloud-native apps run, as expected, in containers; however, these containers are themselves deployed in VMs. On face value, it is less than ideal to deploy apps into containers, which are then deployed in VMs. So why would an operator consider this? If vendors are offering cloud-native 5GC apps, why not go direct to the target platform, shown to the right of the figure, with containers deployed direct to bare metal?

The main reason for this interim phase is that an operator may need to rapidly deploy 5GC but does not yet have a cloud infrastructure platform capable of running containerized workloads that can meet the requirements of mission-critical telecom networks. As an interim step, using the virtualized infrastructure for certain 5GC functions provides assurances that very demanding availability targets will be met. This approach makes it possible to deploy cloud-native 5GC applications (already available from vendors) right away and then migrate rapidly to a cloud-native platform when it is available.

...but rapid progress toward cloud-native

It is also the case that the industry is making rapid progress to the cloud-native architecture shown to the right of the figure. In the case of advanced operators in progressive markets, this transition will be very fast. The infrastructure stack is increasingly mature and hardened, and operators are quickly gaining the skills and operating know-how required to run 5GC on these platforms. Heavy Reading expects cloud-native 5GC deployments to scale rapidly from 2021 onwards.

The move to SA operation using 5GC is clearly of great importance. But to understand how and when this move will affect operators, it must be part of a wider industry transition to 5G networks that incorporates massive investment in radio access network (RAN), transport and cloud infrastructure, with associated management software. To deliver advanced 5G services to business and consumers requires an extraordinary level of systems thinking — and 5GC is a critical component.

Gabriel Brown
Principal Analyst – Mobile Networks & 5G
Heavy Reading

5G MAKES VIRTUALIZATION VITAL, NOT OPTIONAL

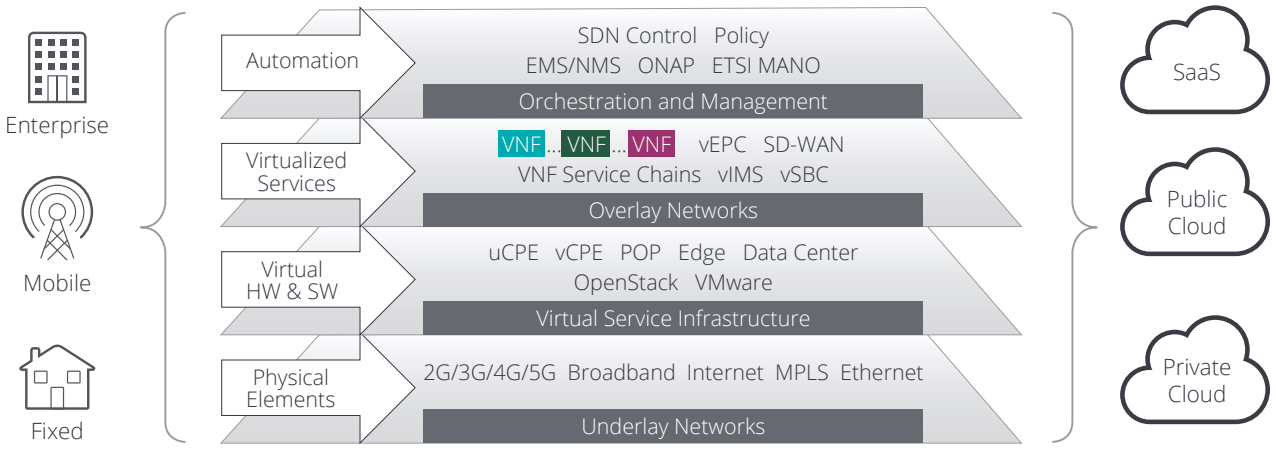
Bruce Kelley
Chief Technology Officer
NETSCOUT

Although the telecom industry has set a course towards virtualization of infrastructure enabled by network functions virtualization (NFV) and software defined networks (SDN), this disruptive strategy is not rolled out comprehensively, writes Bruce Kelley, the Chief Technology Officer (CTO) of NETSCOUT. Leading service providers have embraced the concept of virtualization technologies but still only run relatively low volumes of their total network traffic over their virtual infrastructure.

The reason for this is that immense complexity is involved in the management – or orchestration – of virtualized infrastructure along with interoperation of the underlying traditional network infrastructure. There is enormous fragmentation in these infrastructure with proprietary software and tools being put forward by different vendor systems. In addition, even the open source orchestration landscape has competing options for service providers to select from, adding to the challenges.

The stall in progress of employing virtualization is set to end with the arrival of 5G mobile networks. These projects will provide a stimulus for NFV because the only affordable way to operate 5G networks is to virtualize, change network design, and increasingly manage the network and services from the edge. The affordability challenge is compounded by a shortage of clear use cases for 5G. There's a generalized acceptance that the low latency, high bandwidth of 5G will be of immense use and value

The Complexity Challenge



The Software Defined Data Center - SDDC

in the digitally transforming world but, for service providers faced with multi-billion dollars investments in new network equipment, better-defined business cases are required.

This is not a trivial issue. World Economic Forum/ Accenture analysis, based on data from S&P Capital IQ, estimates that the value of network investments needed to keep pace with demand over the next decade is $2T. Service providers will therefore need to endure substantially increased investment even though 5G profitability is not guaranteed from the use cases that are currently known.

There are, however, a growing number of use cases that can be monetized. Many of these will rely on high levels of service assurance to ensure maximized availability, uptime, and quality. Managing these attributes puts further burden on service providers and comes at a cost. Therefore, increased automation of operations will be required in service management as well as network management.

With consumer 5G devices not expected to come to market until at least 2019, use cases today are related to the core 5G network and include mobile broadband – or fixed wireless access – to deliver 1G connectivity to enterprises. However, depending on the markets they operate in, and the coverage they already have in place utilizing other network technologies, service providers are looking at a spread of different services to provide a return on 5G investments.

Some service providers are looking at massive machine-to-machine (M2M) communication, which will see vast volumes of endpoints requiring connections, although not necessarily all of these will require the performance of 5G. Use cases involving big video such as 4k streaming and use cases that relate to critical or reliable communications that require very high levels of resilience or are reliant on achieving key performance indicators (KPIs), are also being considered. The variety of use cases reinforces the fragmentation of market opportunities and underscores the complexity service providers will need to accommodate in supporting these services over 5G capacity that is also blended with previous generations of mobile and fixed network technologies.

In contrast and more importantly to previous mobile generations, 5G won't be rolled out as a standalone technology and service providers will rely on 4G legacy capacity to support many of the services customers want. The move towards 5G is therefore likely to be a phased migration with areas of population density prioritized. This phased approach adds further management complexity because services will be delivered over a blend of different radio network technologies. Control plane challenges will be heightened by the emergence of network slicing and the complexities of the wider 5G service portfolio.

The 5G new network needs to be flexible and agile with the ability to configure itself to support the demands being placed on it at a given time. In the evening, that might mean ultra-high definition video is supported for users' gaming and video viewing but, during the daytime, this capacity might be focused on enabling collaborative working via unified communications applications. The new virtualized network is expected to spin capacity up and down according to demand.

The new 5G virtualized infrastructure must be automated because the costs of attempting to do this manually would be impossible to sustain within a telecoms business case and there would be no increase in service velocity. This is a key driver for increased uptake of NFV and SDN.

McKinsey has estimated that the newest technologies in NFV and SDN would let operators lower their capital expenditures by up to 40% thereby reducing these costs down to less than 10% of revenues – and their network operating expenses by a similar amount. This illustrates that virtualization technologies are increasingly seen as a savior of a service provider's business, but these insights remain projections and, even though the leading service providers are rolling out the technologies, only a small percentage of traffic is run over virtualized capacity – so far.

In addition, there is some caution as to the extent that virtualization will bring costs down. Last year's Mobile World Live Annual Survey found that 45.2% of respondents think virtualization will bring costs down to a sustainable level but 42.9% are not sure this will happen. There is still more work to be done in communicating the cost benefits of virtualization and, for some, seeing these will be the point at which they believe the promise of NFV and SDN. Until then, virtualization looks to be a difficult and expensive technology to deploy for these organization.

This is the reason why 5G can be a catalyst for NFV and SDN deployment. With use cases for new technologies such as augmented and virtual reality (AR and VR) unclear, service providers are looking to 5G networks to provide enhanced mobile broadband and enable services such as software defined wide area networking (SD-WAN) to justify investment in 5G.

SD-WAN can help service providers generate new revenues because of its ability to instantiate new services flexibly, enabling service providers to provide enterprise services that are further up the value chain than their traditional commoditized connectivity offerings. This is exactly what service providers are targeting because they want to transform their businesses away from providing low value services and provide higher margin, premium services that run on top of their connectivity.

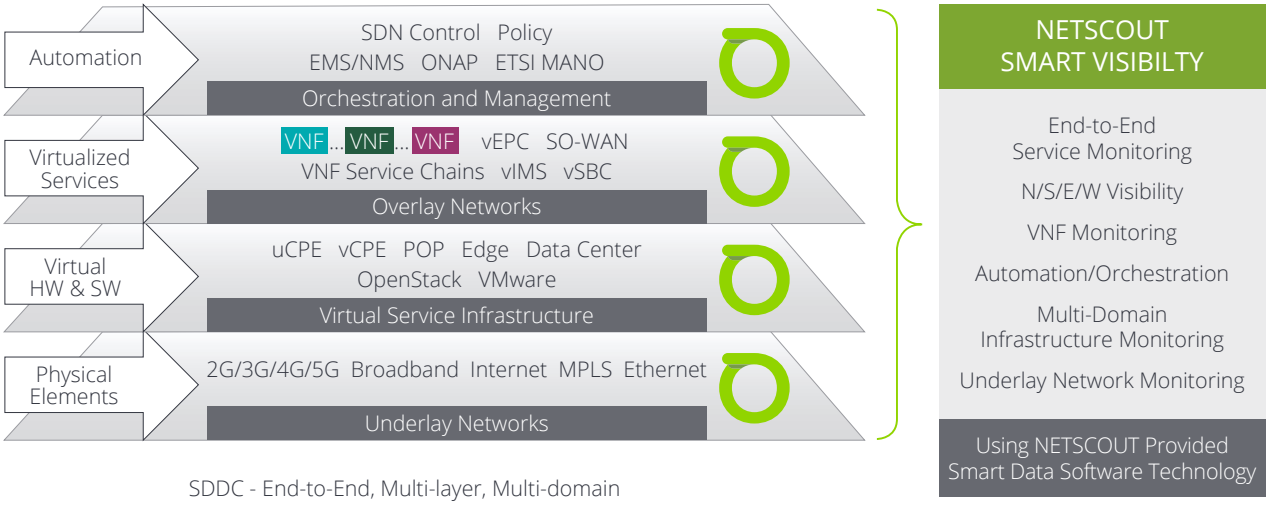
The stakes are high – the digitalization of telecoms could unlock $2T of value for the telecoms industry and wider society over the next decade according to the World Economic Forum. Coincidentally, that figure matches the Forum's projection that service providers need to invest US$2tn over the next decade in their networks mentioned earlier.

With virtualization of the evolved packet core (EPC) and session border controllers (SBC), service chaining, and orchestration plus the move to cloud platforms, the landscape for service providers has become extremely complicated. In addition, it is a new landscape that has moved on from the traditional demands of managing physical infrastructure. Ultimately this new network will be a simpler, highly automated, self-aware network but the challenges of migrating from the traditional environment of physical hardware, manual management, and function specific configuration are substantial.

is vital because of the costs associated with processing vast volumes of irrelevant information.

Fast reacting, accurate unify smart data tools that are aware of the context in which they are operating provide the foundation for service failures to be fixed in near real-time. For organizations that are deploying 5G, for example, there will be added advantages because the technology extends a service provider's ability to understand what's going on in the network and by extension have insight into the performance

The Solution



SDDC - End-to-End, Multi-layer, Multi-domain

What service providers need is smart visibility into this disrupted architecture. This end-to-end, multi-layer, multi-domain coverage can only be provided by software solutions. Traditional tools such as hardware probes are cost prohibitive because they would need to be deployed at every device. However, with virtual probes that produce smart data supported by intelligent tools, service providers can design embedded visibility in to their new networks and succeed in the new telecoms arena.

Virtual probes (with smart data technology) and smart data tools that are "always on" can be relied upon not to miss key data points and deliver actionable insights. These tools incorporate advanced data analytics capabilities and have built-in intelligence to ensure only relevant data – rather than all data – being analyzed. This automated capability

characteristics of any given service. That might be an enterprise SD-WAN service in the early phase of 5G deployment, but it could be a highly monetized consumer service such as ultra-high definition gaming in the near future.

It is business cases like these that will contribute to telecoms and associated industries generating an additional $2T over the next decade. However, to access these revenues in a cost-effective and sustainable way, service providers will need to accelerate their use of virtualized infrastructure to make deployment and operation of enabling technologies – and 5G in particular – viable. 5G needs virtualization to ensure it can be rolled out profitably but virtualization needs 5G too because 5G provides the first opportunity to showcase the advantages of a fully virtualized operational environment.

RESOURCES

NETSCOUT'S WHITEPAPER

NETSCOUT'S industry-proven service assurance, security and big data solutions, fueled by Smart Data, can be leveraged by CSPs for critical phases of the 5G life cycle; which include pre-launch, launch and operations.

GET THE WHITEPAPER

5G READY NOW! DATASHEET

NETSCOUT'S 5G NOW solution for Carrier Service Providers: Gain your competitive advantage on your 5G/ IoT/Cloud Journey with NETCOUT's Smart Data Solution.

READ THE DATA SHEET

INFOGRAPHIC

5 Ways to Get Smart Visibility from Here to 5G

SEE INFOGRAPHIC

ONE SMART QUESTION

What has NETSCOUT learned from working with service providers implementing 5G? NETSCOUT works with service providers all over the world and understands the complexities of implementing 5G networks. With Smart Data, service providers can gain visibility into their 5G networks with NETSCOUT solutions. Heather Broughton, Senior Director of Service Provider Marketing at NETSCOUT, gives insights into three early learnings from 5G deployments.

WATCH THE VIDEO

ULTRA HIGH DEFINITION 5G VISIBILITY. ANY VENDOR, ANY NETWORK, ANY SERVICE

VIEW VIDEO

5G VELOCITY, MEET ULTRA HD VISIBILITY.

ANY VENDOR
ANY NETWORK
ANY SERVICE

NETSCOUT's scalable monitoring solution—designed for the cloud—helps carrier service providers successfully deliver actionable insights into reliability and latency for 5G networks, applications, and services. Our solutions provide secure end-to-end support for both service providers and enterprises.

Future proof with a next generation carrier-grade monitoring software solution and embrace technology challenges with 5G/IoT, the Cloud and beyond.

Go 5G with NETSCOUT's Visibility Without Borders™ at netscout.com/5G

NETSCOUT®

VISIBILITY WITHOUT BORDERS