



4G/5G Private Cellular Networks

What Carriers and Enterprises Need to Know

Matthias D'Autremont & John English



TABLE OF CONTENTS

Executive Summary3

Private 4G LTE – Beyond Wi-Fi and Basic Internet Access3

5G is Here - Are You Ready?4

Why Do We Need Private 5G?4

Flexibility of Private 5G Networks for Enterprises5

5G Network Slicing6

Delivering High Performance Applications6

Multi-Access Edge Compute: The Complexity Explosion6

5G and Your Return on Investment (ROI).....7

5G and Security7

Smart Outcomes for Carriers and Enterprises7

Automation for Private 5G Networks 8

NETSCOUT Analytics Solution..... 8

Conclusion9

Executive Summary

While potentially hundreds of private 5G networks are beginning to be deployed in Western Europe, Asia, and the Americas, it is still in the early stages of 5G deployments - the number of private 4G networks still far exceeds that count. The drivers for private 5G networks are similar to the drivers for 4G networks: realize higher throughput, lower latency, and increase reliability to serve specific application requirements and to protect data. The difference? The 5G standard was created with enterprises in mind.

Manufacturing applications (like smart factories) are leading these private 5G (and 4G) deployments according to an Analysys Mason study (Private LTE/5G network deployments: trends and analysis), but a myriad of new applications for enterprise and government/military enabled by 5G technology are in the planning stages and starting to come alive.

Unlike private 4G networks, enterprises have a wider set of deployment options for 5G private networks, from on premise 5G radio only, to 5G Radio Access Network (RAN) and partial Core, to a full "5G in a box," along with paired Multi-access Edge Computing (MEC) options. Likewise, there are a range of options for the implementation and operation of private 5G networks; with in-house technical expertise (if it exists), and/or with a Network Equipment Manufacturer (NEM), and/or the Communications Service Provider (CSP) or cloud provider, and systems integrator combinations.

The challenge of private 5G is that it presents an increased level of complexity with the new 5G cloud technology for the RAN and the Core, in addition to multiple possible deployment permutations, and multi-vendor solutions. Having independent, holistic, end-through-end visibility is critical to assuring service levels and real-time analytics are meant to feed the orchestration layer for automation as well as to realize private 5G business outcomes.

You cannot guarantee what you can't measure! You need performance visibility and telemetry now more than ever to assure enterprise 5G business services. Mission critical business applications must have measurements that are tuned to the needs of specific service(s) for bandwidth, latency, reliability, and Quality of Experience (QoE). Carriers must guarantee Service Level Agreements (SLAs); especially with continuous latency and bandwidth measurement for smart factory applications, remote surgery, etc. Traditional network latency measurements, based on the three-way Transmission Control Protocol (TCP) handshake, does not work for 5G. Continuous latency and throughput must be tracked to immediately understand, "What, Where and Why" of a latency or throughput issue. Packet data is the best "source of truth" to build that measurement capability. And from packets, Smart Data is constructed to provide actionable intelligence to IT, DevOps, SecOps, Engineering, Marketing, and other functional teams. Partnering with NETSCOUT allows enterprises to embrace 5G Everywhere and provide the leverage needed to Take Visibility Anywhere!

Private 4G LTE – Beyond Wi-Fi and Basic Internet Access

In expansive areas where Wi-Fi connectivity is not adequate, enterprises have deployed Private Cellular Networks (PCN) to manage cost and to support wireless network connectivity, reliability, security, and performance.

There are various architectures and models that supports a PCN including those operated and owned by enterprises or those that are only operated by mobile carriers. Citizens Band Radio Service (CBRS), a lightly licensed cellular service that compliments Wi-Fi with expanded coverage and bandwidth, has been deployed by cable/MSOs and enterprises. New 5G CBRS promises enhanced service capabilities.

Now, PCNs are built extensively on 4G LTE infrastructure and support a high concentration of connected devices with higher latency requirements. But the arrival of 5G, and its edge compute requirements for high bandwidth, low latency, and ultra-high reliability, changes the landscape for PCNs.

The road to private 5G networks was first paved with private 4G LTE, and NETSCOUT is leveraging that experience by reducing the barriers to entry for enterprises using Smart Data visibility. Recent work with a large regional electric utility customer resulted in continuous monitoring of their private 4G LTE network's IoT (Internet of Things) devices, which are critical to quick recovery of power infrastructure issues. The NETSCOUT solution provides Visibility Without Borders into their private 4G network to assure SCADA, 4G LTE control plane, and VoLTE Signaling. This same solution is easily adapted when the customer is ready to transition to 5G.

[Read our Case Study.](#)

5G is Here - Are You Ready?

Technology is evolving and the demand from high bandwidth, low latency applications and millions of IoT devices entering the Wi-Fi access point arena requires increased complexity, faster networks, and higher quality of service. These trends compel enterprises to stay competitive by managing cost, while they continue to innovate.

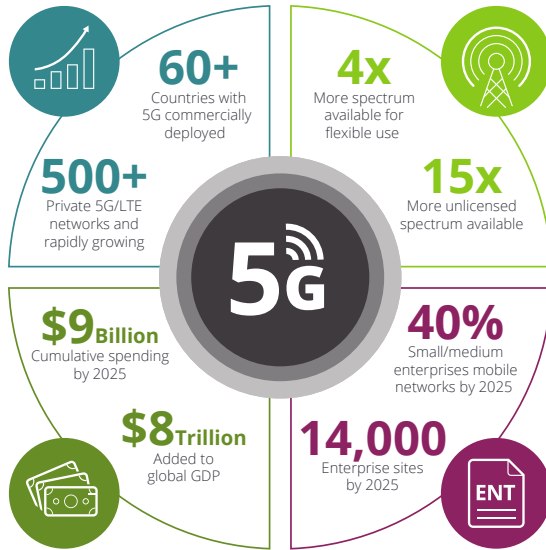


Figure 1: 5G Projected Spending by 2025.

Currently, more than 69 countries have deployed 5G commercially, with over 500 private 5G/LTE networks - a number that is growing rapidly now that life is starting to return to the “new normal.” Fueling the growth of 5G private networks is the availability of 4 times more licensed radio spectrum and 15 times more unlicensed spectrum. The cumulative spending on 5G is expected to reach \$9B by 2025 and in the process, enabling enterprises to add \$8T to the global economy. Of the projected 14,000 total 5G private networks, 40% are expected to be for small and medium businesses by 2025. (Sources: Qualcomm, GSA, Vodafone and Analysys Mason).

Why Do We Need Private 5G?

5G is to businesses what 4G or 3G mobile networks were to consumers! Enterprises will not likely replace Wi-Fi with 5G in “carpeted areas.” But where signal interference is an issue or there is need for broader coverage (more mobility, better security, and device density), private 5G is a complimentary solution. Indeed, Wi-Fi and cable replacement are a fast-growing category because of 5G’s relative cost, flexibility, Quality of Service (QoS) and strong security capabilities. Hundreds of entities are acquiring CBRS Priority Access Licenses (PALs) to build private 5G networks for many industries; for example, to enable “smart” factories of the future where the only things that don’t move are the roofs and the walls. With private 5G there is the opportunity to reinvent business models that have been static for decades. Utilities are building private 5G networks with smart meters and wireless sensors that protect their electric grids. Transmission towers will soon double as weather towers with live stream video. These “smart grids” will help predict customer demand and monitor the impact of weather locally on the grid, providing the capability to instantaneously shut down damaged facilities, so as not to cause further damage to infrastructure and the local environment.

5G is driving productivity by enabling the use of Augmented Reality/Virtual Reality (AR/VR) devices for field technicians. A recent case in the airline industry noted that 5G enabled remote aircraft diagnostics helped saved their business during the pandemic!¹ Private 5G is also enabling new opportunities for remote control of construction and autonomous vehicles. In the US there are over 13,000 mines, many with miles of tunnels and roads. These companies face immense pressure to stay competitive by automating and streamlining costs. Leveraging private 5G, these companies are starting to outfit Automated Guided Vehicles (AGVs) with remote control, tracking, and a myriad of sensors to increase productivity and profitability, while improving analytics and worker safety.

Flexibility of Private 5G Networks for Enterprises

There are many potential deployment scenarios and permutations for enterprise 5G, but they all fall into either a private or public category. For example, if an enterprise needs guaranteed quality of service and exceptional data privacy and security, they may opt for a completely private on-site design. Enterprises can use unlicensed or licensed spectrum leased from a mobile operator. The 5G small cells, 5G Core and MEC can all be on-site. Enterprises can choose to build it themselves and self-manage if they have the in-house knowledge and expertise; or they can partner with a systems integrator, network equipment provider, or mobile operator. On the other hand, if enterprises need lower cost 5G solutions that can be operational quickly but still deliver low latency and good security, they may opt for a hybrid approach, leveraging the mobile operator's RAN or the entire mobile operator network using 5G network slicing. Enterprises can still leverage small cells on premise for coverage and the edge/MEC could be on-premise, hosted, or in the cloud.

The bottom line: there are a myriad of 5G private network deployment options to fit virtually every budget, operational skillset, and data security requirements.

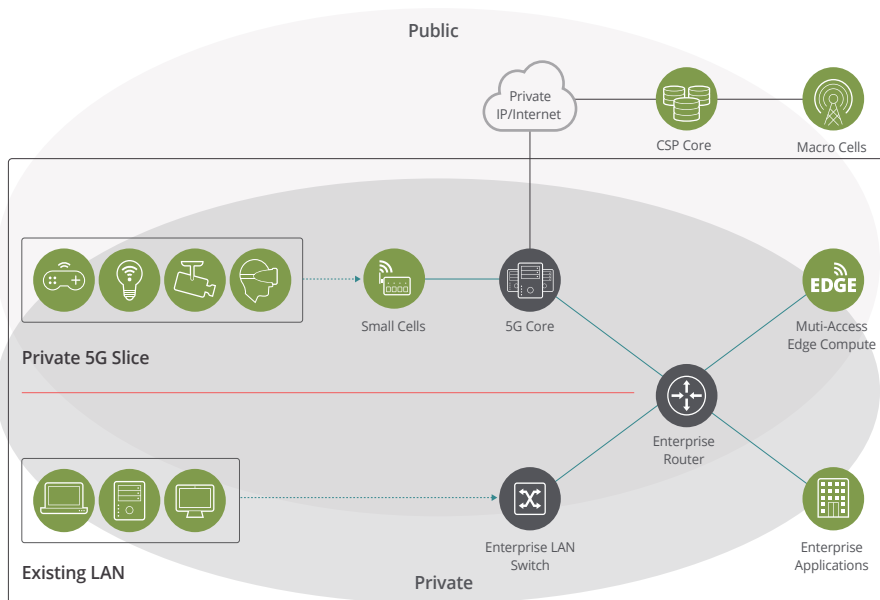


Figure 2: Private 5G LANs – On Site 5G.

¹ [Enterprise IoT Insights, February 2020.](#)

5G Network Slicing

5G network slicing allows mobile operators to provide a virtualized portion of their networks for specific customer or enterprise requirements while optimizing resources and network topology to meet specific SLA requirements such as ultra-reliable connectivity, speed, and capacity for a given application.

While 5G network slicing is still in its infancy, CSPs are likely starting with a handful of fixed slices for applications that require Ultra Reliable Low Latency (URLL) and Enhanced Mobile Broadband (EMBB), Massive IoT (MIoT) gaming, and video. But in a few years, network slices will be orchestrated in near real-time down to the individual enterprise level. If successful, 5G slices may eventually be as common as network domain names! It's also possible to achieve many of the same goals of 5G slicing now, through a distributed small cell or Open RAN architecture, which is less complicated than network slicing.

Delivering High Performance Applications

The advent of Software Defined Networking (SDN) virtualization and orchestration of container-based microservices provide the ultimate deployment: flexibility, scalability, and redundancy for private 5G. CSPs have been working to deliver high performance applications with private 4G LTE but have not been as successful as they will be with 5G. The key to this success is delivering high performance applications through the disaggregation of public cloud and managing the multi-vendor offerings.

While containerized service offerings are becoming the de facto standard for 5G cloud services, they do present their own set of issues with adoption, operation, and security. The need for container-based service visibility is part of end-through-end performance monitoring.

Multi-Access Edge Compute: The Complexity Explosion

MEC decreases the distance - and therefore latency between the User Equipment (UE), or IoT device, and network application elements. For example, a normal 4G mobile communication signal will travel from the UE to the eNodeB and then on to the mobile core in about 100ms, whereas with 5G MEC, that communication is reduced to less than 10ms.

MEC can be connected anywhere near the user or device as needed by the application, device, and service. Mobile devices are routed through the RAN (or traditional wireline network) to the nearest edge compute location. Public cloud is being extended into the enterprise premise with cloud offerings such as AWS Wavelength, Outpost and Azure Edge. Together, 5G and MEC are perfectly suited to deliver high performance applications.



Figure 3: Lack of Visibility Across Architectures.

However, private 5G as a new “edge” or network border means application tiers are spread across on-premise data centers, public cloud, and the MEC on physical and web scale architectures leading to a “complexity explosion.” Lack of visibility for Operations and Engineering teams can lead to poor customer experience caused by slow or failing database queries, SLA violations at the edge, or problems in the RAN - resulting in copious finger pointing for mission critical services. A lag time of more than 50ms no longer feels “authentic;” impacting virtual or augmented reality, gaming, remote surgery, or any/real-time service(s). There’s also massive added complexity from the cloudification of the network and multi-tenancy options for network slicing.

5G and Your Return on Investment (ROI)

To ensure successful deployments and business outcomes, enterprises must have visibility into critical private 5G service performance. Having a powerful and effective proactive monitoring and service triage solution is critical to delivering and maintaining expected 5G service quality. This visibility gives IT Operations teams the confidence to launch new services with the ability to verify and monitor across enterprise sites and public/private clouds. IT teams must have these Smart Data tools to investigate service delivery issues easily and rapidly with guided workflows, as well as perform granular user session tracing and analysis for root cause.

With 5G, service providers and enterprises cannot rely on traditional performance monitoring tools and approaches. New enterprise business services such as smart factories with robotics, remote medical diagnostic, and surgical applications, have demanding service thresholds that must be constantly met. Hence, continuous monitoring of latency and throughput must be provided by the latest generation of performance monitoring tools.

5G and Security

Security has taken on a new focus within Mobile Network Operators (MNOs) as the market and revenue opportunities available from next-generation mobile services running on 4G/5G solidify. There is a new range of threats and concerns for: new enterprises, IoT and Internet of Everything (IoE) services with business, mission and safety criticality aspects, and new higher speed consumer Internet services - with these risks being exacerbated by new technologies, protocols, and platforms of 5G.

Accurate and timely identification of compromised devices is critical to protecting the 4G/5G network from mobile threats. Unlike existing tools focused on IP network visibility where temporary IP addresses must be mapped to subscriber identities retrospectively, NETSCOUT’s security solution, Omnis® Threat Defender, for mobile networks extends its reach directly to the S1-U/N3 interface where data is automatically correlated for control and user plane mapping for the complete end user device identity [phone number, International Mobile Subscriber Identity (IMSI), device type or International Mobile Equipment Identity (IMEI), and IP address] along with the applications and services in use.

Smart Outcomes for Carriers and Enterprises

CSPs face increasing complexity in maintaining and improving the customer experience. They are being asked to meet their customers’ technology challenges for private 5G networks and network slicing as well as cloud migration, automation, 5G, and IoT. At the same time CSPs must deliver new services to monetize 5G investments. Likewise, enterprises are looking to take advantage of 5G technologies to rollout new revenue generating services and accelerate their Digital Transformation initiatives to improve customer experience. And they want to maximize their investments for whatever 5G technology they deploy.

CSPs need to turn traffic information into Smart Data for every 5G technology, vendor, service, and connected device. Smart Data provides actionable intelligence on everything that is 5G, the next G, and beyond. Smart Data is essential to delivering high quality services, reducing churn, and to monetizing networks.

Enterprises are looking to take advantage of 5G technologies to rollout new revenue generating services and accelerate their Digital Transformation initiatives to improve customer experience.

Automation for Private 5G Networks

With the cloudification of the 5G Networks, whether outsourcing development to a vendor or owning this function in-house, IT and CSP Operations and Engineering teams will need new tools to manage the complexity and assure the delivery of 5G enabled services.

With an increasing volume of IoT devices and the distributed nature of edge networks, enterprises and CSPs must consider a real-time monitoring strategy to support 5G-enabled services. To realize both the cost savings and agility 5G networks must have orchestration. Smart Data and the unparalleled visibility it offers help organizations to validate 5G models to continuously optimize network performance in response to traffic fluctuations, enabling a new level of orchestration and automation.

As 5G network functions will need automation, it is expected that Network Data Analytics Function (NWDAF) will become essential to the operation of 5G networks in the near term. The NWDAF is a new 3GPP defined analytics function in the 5G Core network used to collect data from user equipment, network functions, application functions, and operations and management (OAM) systems, etc. from the 5G Core, Cloud, and Edge and RAN networks that can be used for analytics. Smart analytics will be needed for the new 5G Core NWDAF, and to realize the goals of a self-optimizing network with 5G, CSPs must have real-time, end-through-end network service intelligence to inform the orchestration layer for automation.

NETSCOUT Analytics Solution

Artificial Intelligence and Machine Learning combined with the power of NETSCOUT's Ultra High-Definition Smart Data and deep domain knowledge delivers Smart Outcomes for CSPs. CSP Business Operation groups can now harness this automated power to gain actionable business intelligence into their top end-to-end network voice and data challenges with NETSCOUT Analytics solution.

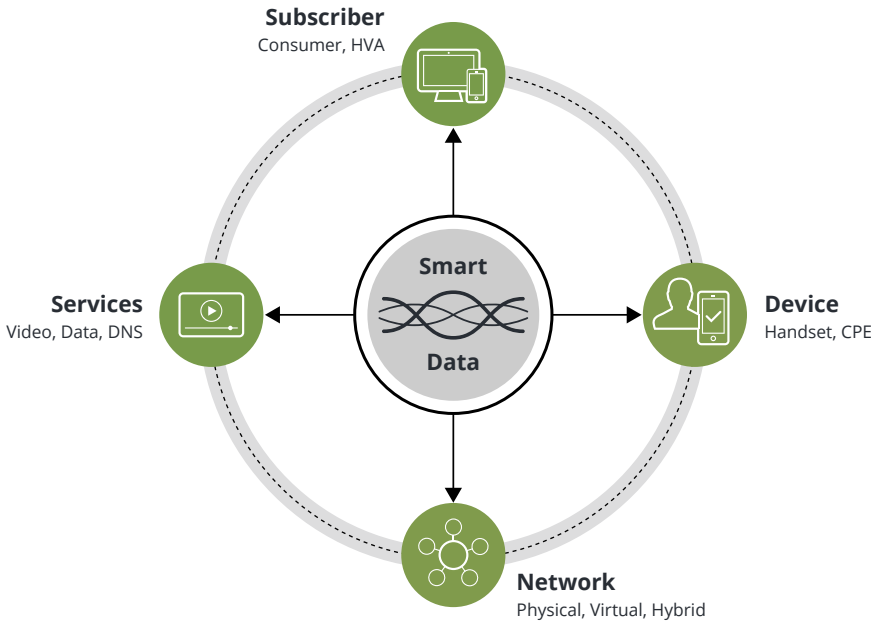
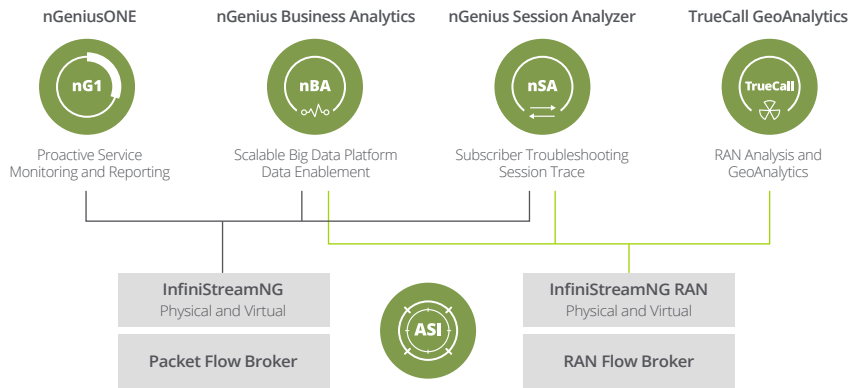


Figure 4: Ultra High-Definition Smart Data.

Modern End-to-End Analytics Solutions for Service Providers and Enterprises



LEARN MORE

For more information about NETSCOUT solutions visit:

www.netscout.com

www.netscout.com/5G

www.netscout.com/solutions/enterprise-5g

Now, with NETSCOUT's Analytics solution, CSPs can work with Enterprises to gain Smart Outcomes and can:

- Automatically pinpoint Business Operations' top issues and where they need to focus – providing actionable business intelligence in the most impactful areas.
- Automate workflows - saving thousands of operational hours.
- Gain automatic insights into service degradation; detecting outliers, the number of subscribers being impacted, individual subscribers who are being affected, and then prioritizing subscriber tickets - lowering MTTR (Mean Time To Repair).
- Discover unmet service needs and opportunities.

Conclusion

Whether the private 5G network is located on premise, off-premise, or a hybrid of those – having end-thru-end service visibility is critical to assuring customer experience and monetizing device and end user behavior. NETSCOUT solutions provides this visibility to continuously deliver timely and valuable insights across RAN, Edge, and Core; enabling users to explore real-time scenarios, create custom KPIs, and drive informed business decisions using Smart Data. Private 5G has the potential to transform the world as we know it. But the complexity multiplication requires Visibility Without Borders.

With NETSCOUT you have a trusted proven partner to minimize risk and prepare for success - partnering with NETSCOUT will allow enterprises to embrace 5G Everywhere and provide the leverage needed to Take Visibility Anywhere!



Corporate Headquarters
 NETSCOUT Systems, Inc.
 Westford, MA 01886-4105
 Phone: +1 978-614-4000
www.netscout.com

Sales Information
 Toll Free US: 800-309-4804
 (International numbers below)

Product Support
 Toll Free US: 888-357-7667
 (International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us