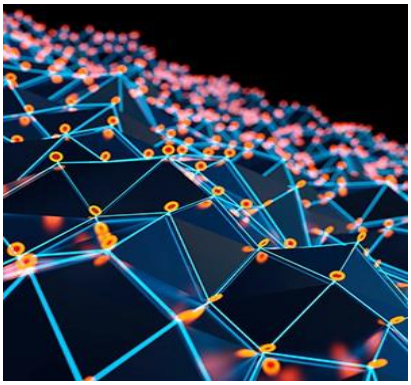
www.pipelinepub.com
Volume 21, Issue 2

Why Private Network Assurance Needs a Holistic Approach

By: Nicolas Timothee



Private networks have become indispensable for enterprises that require secure, high-performance, and reliable connectivity. According to Analysis Mason, global spending on private LTE and 5G networks is projected to reach $9.2 billion by 2028. However, building and maintaining successful private networks require more than just infrastructure; they demand a holistic approach emphasizing proactive management and complete visibility. There is an old adage that says, “You can’t control what you don’t see,” and it is particularly true in this context. Private network operators need actively managed networks to support the complex requirements of mission-critical operations.

Drivers for Private Networks

The adoption of private networks is driven by a combination of needs: mission-critical system reliability, operational efficiency, and enhanced security.

Mission-Critical Systems: Private networks are essential for industries where uninterrupted service is crucial. For example, an unexpected network outage in large airports that halts communication for just five minutes can result in planes idling on the tarmac, delaying operations and costing millions. In such settings, private networks ensure low latency and high availability, allowing systems like real-time logistics, baggage handling, and ground crew communication to function seamlessly.

Operational Efficiency: Private 5G networks enable real-time data processing, which is essential for the smooth operation of connected devices and automated machinery. Unlike public networks, private 5G networks offer complete control over data routing and resource allocation, making them more suitable for environments with heavy data requirements, such as smart factories. These networks support instantaneous data transfers, enabling quicker decision-making and faster response times, boosting productivity and agility across an enterprise.

Security and Control: Enterprises seeking higher security and data control levels often opt for private networks rather than relying solely on public communication service providers (CSPs). While CSPs can provide reliable and broad coverage, they cannot match, at least for now, the customizable security features of a dedicated network. Private networks allow enterprises to implement advanced security protocols, such as zero-trust architecture and specialized encryption, reducing exposure to potential threats. This capability is vital for industries that handle sensitive data, including healthcare and finance.

Enterprises may choose private networks over public CSP reliance for several reasons:

- Custom Network Management: Tailored network settings allow businesses to prioritize and secure mission-critical applications.
- Data Sovereignty: Full control over data ensures compliance with industry regulations and minimizes risks of external breaches.
- Dedicated Resources: Unlike public networks with shared bandwidth, private networks guarantee dedicated resources, ensuring consistent performance even during peak demand.

The Influence of Standards on Private Networks

The standards set by 3GPP have shaped the evolution of private network capabilities. These standards guide how CSPs and private network operators deploy and enhance their network services.

Current Challenges with Standards

While 3GPP Releases 15 to 17 introduced crucial capabilities like enhanced mobile broadband and basic network slicing, they still need to fully address the specific needs of large-scale, high-stakes private networks. CSPs operating on shared infrastructure face limitations in customization and data isolation, which can hinder their ability to support industries with rigorous performance and security requirements. The introduction of 3GPP Release 18, 5G-Advanced, brings enhancements that significantly improve network capabilities. These include:

Expanded Network Slicing: The ability to allocate specific service levels to different network segments ensures high performance for priority applications.

AI and Machine Learning: Integrating AI and machine learning improves network automation, predictive maintenance, and real-time optimization, enabling more responsive and adaptive network management.

Support for Advanced Use Cases: New features support applications like augmented reality (AR) for training, digital twins for operational simulations, and enhanced IoT functionality for connected devices.
These advancements will enable CSPs to support enterprise needs better. Only with these capabilities can CSPs now start to support some of the most demanding requests from their largest enterprise customers. On the other hand, private network operators can use these standards to build even more customized and resilient systems that align with their specific operational demands.

Different Setups for Private Networks

The variety of private network setups available underscores the need for a holistic approach. Each configuration has complexities and requirements that must be tailored to the specific use case, as follows:

On-Premises Networks: These networks provide the highest level of control, making them suitable for environments that demand rigorous data protection and low latency, such as hospitals or manufacturing plants. However, on-premises networks require substantial investment in setup and maintenance.

Hybrid Private Networks: Hybrid networks combine on-premises and public infrastructure and offer a balance of high security and scalability. They are ideal for organizations with distributed operations or those requiring localized control and broader connectivity.

Managed Private Networks: Smaller enterprises may choose managed private networks for their ease of use. While this setup outsources some network control, it still offers dedicated resources and greater customization than public CSPs. However, the ability to respond to mission-critical issues may be limited compared to entirely in-house management.

Geographically Distributed Networks: Enterprises with operations in different locations face unique challenges. Managing consistent performance and security across dispersed facilities can be difficult, particularly when integrating multiple network types, such as private 5G, LTE, and Wi-Fi. These situations require specialized solutions to maintain seamless communication and performance.

Complexities and the Need for Custom Solutions: Managing diverse network setups involves integrating various technologies, handling geographic differences, and aligning with industry-specific regulations. For example, a rail system operating across multiple countries may need to adhere to different safety and operational standards, impacting how its private network is configured. Similarly, hospitals with multiple campuses might need different network capabilities depending on whether a facility is focused on critical care or outpatient services. This diversity highlights why one-size-fits-all solutions do not suffice and why a holistic, adaptable approach is necessary.

Use Cases from Various Industries

Airports exemplify environments where private networks must operate flawlessly. A network outage impacting ground services, real-time communication, or baggage handling can lead to flight delays, passenger dissatisfaction, and significant financial losses. Keeping network assurance in-house allows operators to maintain the flexibility and speed needed for rapid response and problem-solving. Other industry examples include:

Healthcare: Hospitals rely on private networks for secure, continuous patient monitoring and data exchange. The network requirements for a high-capacity urban hospital differ from those of a minor clinic, yet both need low-latency, high-reliability connectivity.

Transportation Systems: Rail networks use private networks for signalling, train schedules, and communication with control centers. These systems require consistent performance across long distances and through varied environmental conditions.

Manufacturing: Factories depend on private networks to support automated assembly lines, IoT sensors, and machine-to-machine communication. The network must be robust enough to handle high data traffic and responsive enough to support real-time adjustments.

Advice for Private Network/Enterprise Customers

Understanding your specific operational needs is essential for enterprises considering private network deployments. Start by identifying mission-critical systems and prioritizing them in your network design. Whether you require ultra-reliable, low-latency communication for real-time services or heightened data security for compliance, having a clear set of requirements will shape the most effective network strategy.

It’s also crucial to plan for scalability and adaptability. Private networks should be capable of evolving with your business as operational demands shift or new technologies emerge. Investing in solutions that leverage future-proof standards, such as upcoming 3GPP releases with advanced features like network slicing and AI-driven automation, will keep your network agile and prepared for change.

Visibility into network operations cannot be overlooked. Comprehensive monitoring tools that provide real-time insights are essential for ensuring uninterrupted performance and pre-empting potential disruptions. This is especially true for industries where uptime is non-negotiable. Consider whether your organization has the expertise to manage the network in-house or if a hybrid approach with externally managed services would be more effective for your needs.

Security should be a top priority in your network strategy. Implement robust protocols, such as zero-trust frameworks and end-to-end encryption, to safeguard sensitive data and comply with regulatory standards. These measures help mitigate the risk of breaches and bolster trust in your network’s resilience.

Advice for Vendors

Vendors offering effective private network monitoring and assurance solutions must embrace complementary partnerships and collaboration. Working closely with other technology providers and industry stakeholders helps create an ecosystem that supports seamless network oversight and proactive assurance. This cooperative approach allows for developing comprehensive solutions that address

complex customer needs.

Understanding the unique challenges and needs of enterprise customers is just as important. Vendors should invest time in learning their clients' specific operational environments and concerns, whether it's a large airport's real-time connectivity needs or a healthcare facility's stringent data protection requirements. Tailored solutions that reflect industry-specific demands can better serve these sectors and build stronger customer relationships.

Developing assurance tools incorporating AI and machine learning is also key, though those capabilities would be a Stage 2 activity or beyond for many private networks. Advanced technology allows for predictive maintenance, real-time optimization, and adaptive network management, supporting customers in maintaining high network performance under various conditions. Offering tools that provide thorough health assessments, performance insights, and real-time device/subscriber views will significantly impact.

Any monitoring solution should be flexible and scalable, taking data from many sources. Vendors must design products to support diverse network configurations, including on-premises, hybrid, and geographically distributed networks. This adaptability ensures customers can expand or adjust their network setups without sacrificing control or visibility.

Finally, aligning with industry experts' knowledge can elevate a vendor's offerings. Sector-specific insights enable vendors to create assurance solutions that are technically robust and aligned with operational and regulatory standards. Building trust through collaborative, informed solutions will demonstrate a commitment to the customer's success and pave the way for long-term partnerships.

In summary, enterprises considering private networks must approach their deployment with a clear understanding of their specific needs, ensuring comprehensive visibility, scalability, and robust security measures. Active management and tailored solutions are vital to support mission-critical operations and maintain high performance. Vendors should prioritize partnerships and collaboration to develop flexible, AI-integrated assurance tools while gaining deep insights into customer requirements to provide solutions that align with industry-specific standards.

This approach ensures that private networks are monitored effectively and optimized for resilience and adaptability. By focusing on these principles, enterprises can confidently harness the full potential of their private networks. At the same time, vendors build trust and long-term partnerships by aligning their services to the real needs of their clients.