

WIRELESS PRIVATE NETWORKS: HOW PRIVATE IS PRIVATE?

What to look out for when choosing a wireless private network for your organisation





■ Private wireless is having a moment – but not all networks are as private as they seem

79% of organisations reported a **10% or greater** reduction in emissions after deploying a wireless private network

Nokia 2024 Industrial Digitalization Report

Across all industry sectors, organisations that rely on connected devices are increasingly opting to install a wireless private network on their premises.

Rather than transferring data over the same public 4G and 5G networks that we all use as consumers, they're choosing to invest in their own, private versions of those networks.

Wireless private networks offer many benefits, like faster data transfer, enhanced security, lower costs and reduced emissions. But not every solution marketed as a wireless private network is fully private, and buyers should be watchful when evaluating and choosing solutions.

In this guide: when is a wireless private network truly private?

This guide is designed to help you gauge how private your prospective wireless private network is, and whether it offers the functionality your organisations really needs. We'll cover:

- What is a wireless private network?
- How does a fully-private network differ from a public and partially-private network?
- What are the business benefits of installing a fully-private wireless network?
- What sorts of organisations can benefit most from a fully-private wireless network?

We'll finish with 10 questions to ask when evaluating a wireless private network solution.

■ What is a wireless private network?

A wireless private network is a private version of the public 4G, LTE, 5G, or CBRS networks that our smartphones connect to daily.

It uses the same technologies as these mobile networks, but it's installed for use by a single organisation, and is only accessible to devices registered on the network. It's also managed by an expert partner, eliminating the need to attract and retain costly talent.

A fully-private, managed network offers many advantages over public cellular networks:



Designed, evolved and scaled to your requirements

Your managed network partner will build, manage, evolve and scale the network in line with your own requirements, ensuring your needs are covered now and in the future.



Optimised speed and capacity

A wireless private network can scale to accommodate high densities of devices and high volumes of data, meaning it remains highly performant even at times of peak data transfer. That's essential if your business relies on continually exchanging high quantities of data between devices, sensors and servers.



Low latency

The short distances between devices and servers means there's only a millisecond-level delay between data being generated, a server processing it and issuing an instruction, and a device receiving the instruction and acting on it. That's vital for latency-critical use cases like remote control of equipment.



Coverage

A wireless private network can ensure that all areas of your site—indoors and outdoors—are adequately covered. This can ensure connectivity in areas that have been hard to connect previously, or where public cellular network signals may be degraded.



Security

As a closed, managed system, a wireless private network offers greater security than having your sensitive data travel across public cellular infrastructure. Only authorised devices can access it, reducing the risk of attacks and data breaches.



Reliability

A wireless private network maximises reliability for business-critical operations by eliminating risks like coverage dropouts and peak-time congestion. It's also typically backed by an SLA from the managed network partner, assuring high levels of uptime and availability.

■ How does it differ from a public cellular network?

A truly private wireless network is a self-contained system, with all of the infrastructure installed on your own premises and managed for you by your chosen network partner. While the network architecture will vary depending on the organisation's needs, there are three core elements:



Devices

SIM-based authentication ensures that only authorised devices can connect to the network.



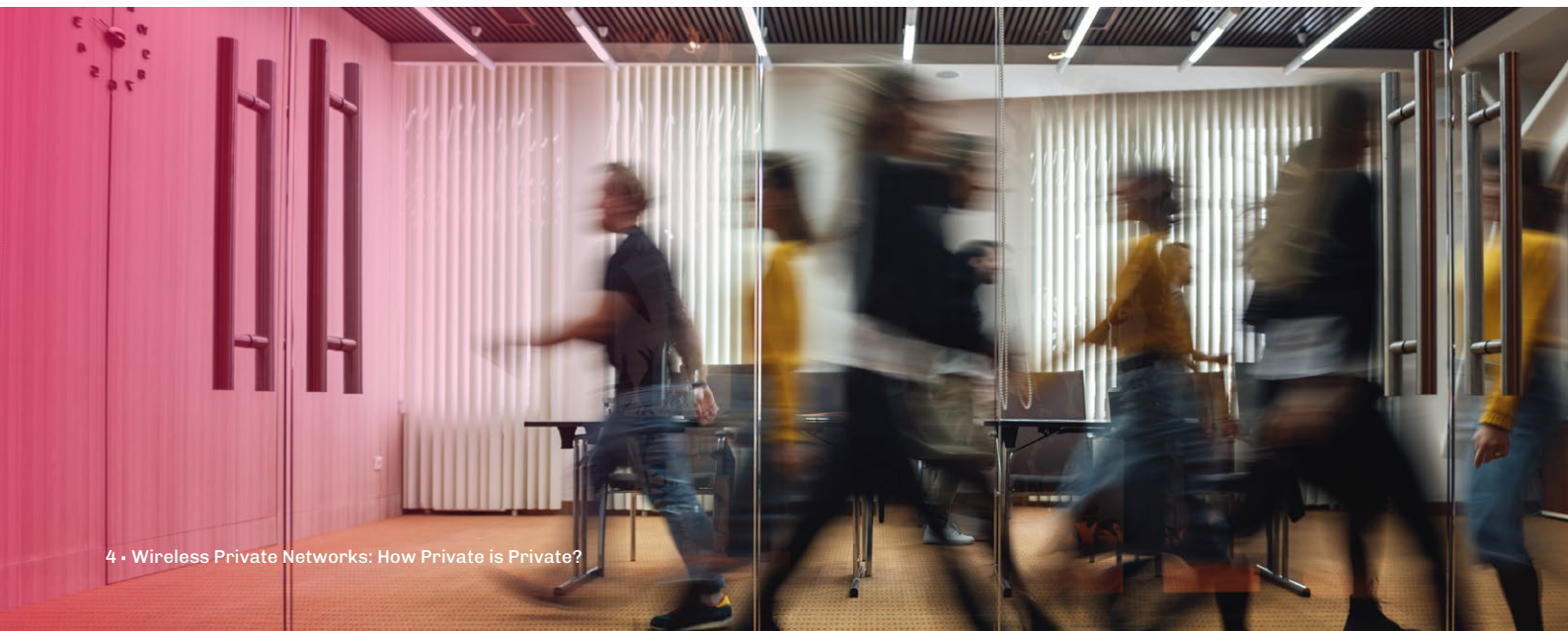
Network

A wireless private network typically consists of an access network (the radio antennas that devices connect to), the packet core, which routes the data through the network, and edge compute that processes the data on-site. Crucially, it is physically and logically isolated/separated from other networks, especially public mobile networks.



Security

While the exact security architecture will vary depending on the needs of the organisation, typically it will include end-to-end encryption to protect data in transit, network slicing or dedicated spectrum to prevent interference and unauthorised access, and customisable firewalling, intrusion detection, and access control policies.



■ When is a private network not a private network?

When evaluating a private network solution, it's important to understand whether all of the network elements are private and dedicated to your own organisation.

Some partially-private or hybrid solutions carry your data across a public cellular network for part of its journey. This means your network may be at risk of congestion and your data may not always be fully segregated from other network users, exposing your network to threats and impacting performance.

In this instance, it also means that if the public network has a fault, your own network will be impacted; unlike a fully private network that operates separately and will continue to function even if a nearby mobile network isn't working.

Public-private hybrid network architecture models

With public-private hybrid network architecture models, elements of the network are hosted on site; others sit within the public mobile network.

This means that data traffic has to pass between the public, shared, network and the on-site network elements.

Neither end-to-end security nor performance is guaranteed.

Dedicated private networks

But, in the case of fully private networks, all infrastructure is installed on-site, and all traffic remains on-site.

This means that no private traffic mixes with unsecured, unknown traffic. Plus, security and performance are assured end-to-end.

■ Why invest in a fully-private wireless network?

As a dedicated custom network just for your organisation, a fully-private wireless network may sound like an expensive option.

But if you need to transfer large quantities of mission-critical data across one or more sites, it can deliver significant cost and operational benefits over and above providing the necessary performance and security.

Among the benefits reported by respondents to Nokia's 2024 Industrial Digitalisation Report were:

- **ROI in 12 months:** While wireless private networks can represent a significant investment, almost all (93%) respondents said they achieved full ROI on their private network deployment within a year. A large majority (80%) reported positive outcomes within six months, and a sizeable minority (25%) achieved ROI after just one month.
- **Enhanced business continuity:** Much of the reported ROI was a result of improved business continuity. An always-up, always-reliable network means connected equipment can run without a hitch. It also supports initiatives like predictive maintenance, designed to prevent downtime.
- **Improved worker safety:** A wireless private network can support digital safety initiatives like self-monitoring equipment, wearable alarms, remote control, and robotics and drones for access to hazardous spaces. Almost two-thirds (65%) of Nokia's respondents saw a 10% or greater improvement in worker safety after deploying a private network.
- **Greater sustainability:** Private networks support the continuous collection and analysis of environmental data like CO₂ emissions, air quality and water pollution, enabling timely action. Over three-quarters (79%) of organisations surveyed by Nokia reported a 10% or greater reduction in emissions after deploying a private wireless network.



■ What sorts of organisations benefit most from a fully-private network?

A fully-private wireless network has most value for organisations that are investing in technologies like site-wide IoT deployments, autonomous vehicles, remote controlled equipment and real-time monitoring and analytics. Sectors that can benefit particularly include:



Manufacturing

Private networks support Industry 4.0 initiatives like enhanced automation, predictive analytics, and real-time modelling. Key uses cases include:

- **Autonomous mobile robots (AMRs):** AMRs need to navigate and co-ordinate in real time across the factory floor. The ultra-reliable, low-latency connectivity offered by the private network ensures safe and efficient navigation in dynamic environments.
- **Predictive maintenance:** Predictive maintenance relies on sensor-equipped machinery that can report anomalies and trigger alerts before failures occur. Supported by a private network, real-time data collection and analysis can reduce unplanned downtime and extend equipment lifespan.
- **Digital twins:** Many digital twins import real-time data into virtual models of production lines for simulation and optimisation. A private network supports the high-speed data synchronisation required for accurate virtual modelling for process optimisation and scenario testing.



Logistics and warehousing

In a large warehouse environment, a private network can help to improve safety, efficiency, and inventory accuracy. Key use cases include:

- **Automated guided vehicles (AGVs):** AGVs need to be able to plan routes around the site and avoid collisions. Seamless, low-latency communication via a private network supports precise movement and coordination, improving throughput and safety.
- **Inventory tracking:** RFID tags and IoT sensors provide real-time visibility of stock levels and locations. Private networks enable real-time visibility of stock via continuous sensor data collection and analysis – helping to reduce errors, shrinkage, and manual labour.
- **Smart loading bays:** Synchronised vehicles, gates, and warehouse systems can reduce turnaround times and improve scheduling accuracy – resulting in higher efficiency and lower operating costs. A private network supports the real-time synchronisation required.



Healthcare

Digital healthcare initiatives supported by a private network can enable surgical precision, improve asset visibility and lead to better patient outcomes. Key use cases include:

- **Connected medical devices:** Connected devices can improve patient care in a hospital setting by continually monitoring vital signs and other indicators, and allowing consultants to access information without having to leave the patient's side. Continuous, secure monitoring enabled by a private network improves patient outcomes and reduces admin.
- **AR-assisted surgery:** Smart glasses can replace bulky screens and allow clinicians to access imaging and data that help make surgery more precise. A private network can provide the low latency and high reliability necessary for real-time visualisation and precision.
- **Asset tracking:** Critical equipment like ventilators and infusion pumps can easily go missing in large facilities. Rapid location of critical equipment enhances operational efficiency and emergency response.



Energy and utilities

Private networks offer many benefits for utilities and energy suppliers, including improved grid resilience, safer inspections, and enhanced worker protection. Key use cases include:

- **Smart energy generation:** A private network with IoT sensors can ensure plants are operating as expected, and support predictive maintenance to address any issues before they arise. Such real-time capabilities improve grid stability, reduce outages, and support renewable integration.
- **Remote inspection:** Private networks and video-equipped drones can make inspection more efficient and remove humans from hazardous situations. Remote inspection of pipelines, turbines or solar farms reduces fuel costs and improves safety.
- **Worker safety:** In areas of elevated risk, wearables and sensors can detect hazards early, triggering alerts and emergency protocols. A wireless private network can ensure alerts are received and acted on instantaneously.



Transportation and smart cities

Multi-site wireless private networks are a key component of many smart city initiatives, supporting improved traffic management, safer transit, and enhanced emergency readiness. Key use cases include:

- **Traffic management:** Real-time data from cameras and sensors can feed into dynamic signal controls that optimise traffic flow and reduce congestion. A private network enables data to be collected and acted upon without a hitch.
- **Connected public transport:** When a private network enables buses and trains to seamlessly communicate with infrastructure, it can improve scheduling, enhance safety, and elevate the passenger experience.
- **Public safety networks:** In a crisis, emergency services and first responders need to be able to communicate and co-ordinate a response. Private networks support dedicated, secure communications to ensure all parties can act swiftly and effectively.



Education and campus networks

Educational institutions can benefit from wireless private networks to support immersive learning, keep research data secure, and enable sustainable campus operations. Key use cases include:

- **AR/VR learning environments:** Immersive educational experiences can enhance engagement and retention, but only when they work without a hitch. A private network can ensure the high bandwidth and low latency needed for immersive, interactive experiences.
- **Secure research networks:** Researchers working with sensitive academic or scientific data need to be able to communicate and share information in a highly secure environment. A private network can keep data ringfenced and protected wherever it goes.
- **Smart campus systems:** Smart technologies like automated lighting, HVAC and security controls can reduce operational costs, lower energy consumption and enhance safety. A private network can ensure that smart systems operate smoothly everywhere on campus.



■ 10 questions to ask when choosing a wireless private network

If you're considering investing in a wireless private network, these 10 questions are worth putting to prospective providers. They will help you to assess how private the solution on offer is, so you can weigh the pros and cons of a fully-private or hybrid network solution.

1

How much control and visibility will we have over the network?

This is a good question if performance visibility and control are important to you. Some hybrid networks may depend on the mobile operator to make changes, limiting your own control, scalability, and visibility.

2

What happens if there's a problem with the network?

A fully-private network will come with dedicated expert management and SLAs to ensure any problems are addressed as soon as they arise. A hybrid network may require you to raise tickets and wait in line for help with a fault.

3

What if our needs change as our business evolves?

A fully-private network is built to your requirements, and your provider should be ready to flex and scale it as your needs change – usually discussed in regular service reviews. A hybrid network is typically less flexible as it's constrained by the operator's network capabilities and policies.

4

Will the whole network be for use by our business only?

Fully-private networks have infrastructure that's dedicated to your business. Hybrid networks typically have shared elements, such as the RAN and/or packet core functions.

5

Will the network be fully secure and restrict unauthorised access?

A fully-private network will have high security standards and no unauthorised external access. A hybrid network may also have high security standards, but your data will traverse the public internet via the operator's network.

6

Who owns and controls the network's elements?

Private network solutions may range from dedicated infrastructure with no components that lie out of your control, to a hybrid network with some shared/public elements, limiting your control.

7

How much experience does the provider have with similar private networks?

Specialist providers will have years of private networks experience across multiple geographies and vertical markets. This often gives them the edge over mobile network operators (MNOs) who may lack specialist knowledge.

8

Will the network support mission-critical voice and video applications?

If you need guaranteed performance for voice, video and/or automation, choose your network provider very carefully. While a dedicated private network can deliver high speed and low latency to your requirements, a hybrid network is constrained by the performance levels of the MNO's network.

9

How secure will the network be?

Truly private networks have high levels of security and privacy due to dedicated infrastructure and strict access controls. Shared infrastructure frequently offers moderate security and privacy, as the network shares infrastructure and security measures with the public network.

10

Will the network be interoperable with our other networks?

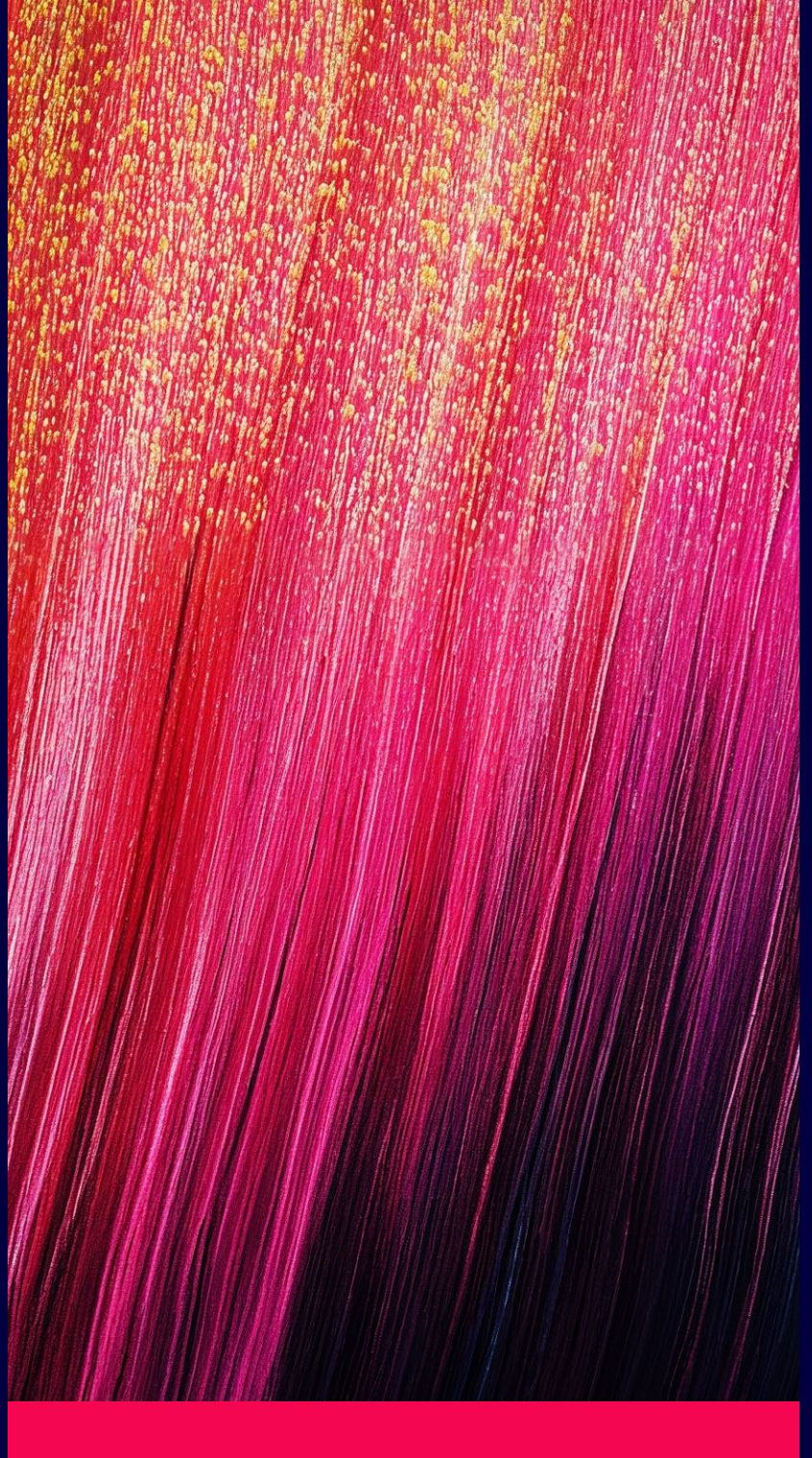
A dedicated private network can be designed to be highly interoperable with other networks, giving you more freedom and flexibility in vendor choice. A hybrid network may limit your hardware choices to ensure tight integration with the operator's public network.

Boldyn: An experienced partner for your wireless private network

In this guide we've discussed the important distinction between fully-private and partially-private or hybrid wireless networks.

We've shown how fully-private networks are better placed to support organisational needs for bespoke architectures, network performance, cybersecurity and future network evolution. We've also suggested 10 questions to ask prospective providers to ensure you're investing in the right solution for your needs.

Boldyn Networks has been designing, deploying and managing fully-private, dedicated wireless networks for customers worldwide for over 10 years. If you have any questions arising from this guide, we'd be delighted to help.



Boldyn Networks delivers the advanced shared network infrastructure needed for a smart, inclusive, and sustainable future. We enable connected transit, venues, enterprises, heavy industry, college campuses and smart cities to create new possibilities in the way people live, work and play.

We don't just talk about the future. We exist to help build it. Creating the foundation from which a better collective future can be imagined.

To learn more visit **boldyn.com**