WHITE PAPER

Why CIOs should consider Private Wireless

Dean Bubley

Disruptive Analysis

Don't Assume

celona

Contents

Executive summary	3
Private Wireless key purposes and use-cases	4
Top 3 Use Cases for Private Wireless	5
Private wireless drivers, enablers and challenges	10
Delivery, architectural and deployment models	13
The implementation process and ongoing management	16
CIO decision-making considerations and criteria	17

© Copyright 2023 Celona Inc. All rights reserved.

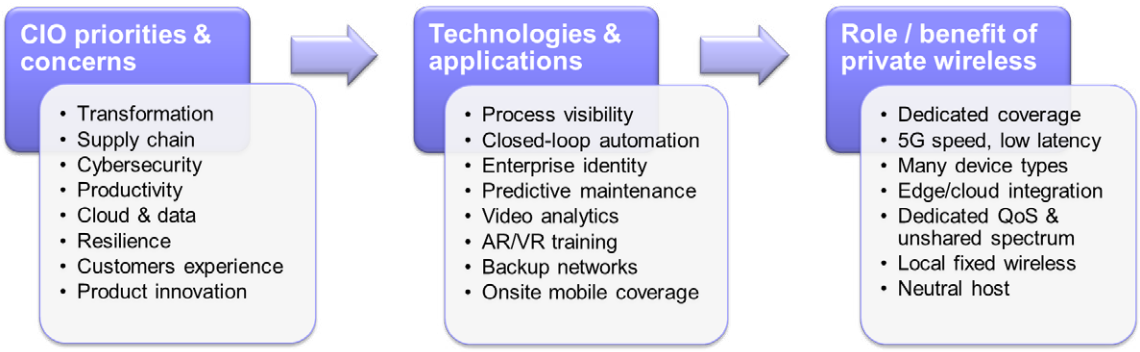
Executive summary:

CIOs should strategically prioritize the integration of private wireless technology.

Private wireless, particularly private 5G networks at enterprise sites, is a strategic technology trend that CIOs need to plan for. It offers various new applications and capabilities for businesses, government bodies, and communities.

Private 5G networks have transitioned from being niche solutions since around 2000 to becoming mainstream for enterprises. This shift is driven by factors such as the availability of enterprise-suitable 5G equipment and software and the need for reliable and flexible wireless systems.

Private wireless networks align with CIOs' overall technology strategy and architecture responsibilities, including productivity, innovation, and supply-chain transformation. They are well-suited to key technology trends like cloud, AI, and cybersecurity, as well as sector-specific technologies like industrial automation and connected vehicles



There are currently over 1000 large-scale private wireless systems in operation globally, with the expectation that this number will grow significantly (possibly 10x to 100x) by the end of the decade. These systems are already in use in over 30 countries with a wide range of applications and use-cases.

CIOs face various decisions when implementing private wireless, including partner selection, the choice between single-vendor solutions and custom integrations, and how to link the private network to existing IT/OT systems. The report highlights the direct connections between CIO priorities and the maturation of private wireless technology and how they can be leveraged.

© Copyright 2023 Celona Inc. All rights reserved.

Private Wireless key purposes and use-cases

This segmentation of private wireless runs alongside "vertical industries" as a way to divide it into sectors. While convenient in terms of framing market and business drivers, any given vertical has dozens of sub-categories and hundreds of applications and deployment scenarios. For instance, the "energy vertical" covers everything from a gas station, to an offshore windfarm, a 1000km pipeline or an oil-futures trading floor in a financial district.

CIO concern / priority	Examples of tech & application evolution	Private wireless Role
1. Industrial transformation	IoT sensors for closed-loop, realtime automation	Wide coverage, support of many device types, OT integration
	Remote visibility and control	Wireless handhelds enabling oversight anywhere on campus
2. Cybersecurity	Enterprise-controlled identity and authentication	Corporate-issued SIM / eSIM and permitted user registry
	Radio interference / jamming	Licensed spectrum & higher power of private 4G/5G vs WiFi
3. Productivity	Improved connected vehicles, robots & AGVs	24x7 operation. Human controllers centralised to oversee multiple endpoints
	Preventative maintenance	Realtime telemetry of asset performance & condition
4. Cloud strategy	Need for hybrid- + multi-cloud access across multiple sites	Local breakout, direct cloud on-ramps + integrated network/edge compute
5. Geopolitics	National focus on industry 4.0, tech sovereignty & connected military / safety forces	Increasing awareness & focus by policymakers on local / campus / indoor connectivity
6. Supply chain / reshoring	End-to-end asset tracking and supply chain management	Connected and automated warehouses, ports & logistics centres
7. Data & analytics	Distributed data collection and analytics	Integrated private wireless & edge-compute nodes
8. IT/OT agility & scalability	Modular & reconfigurable factory layout & processes	Each industrial "cell" connected with wireless vs. fixed fibre
9. OP Indicator 1	Adding incremental applications to existing infra	Use-case stacking and ability to use QoS mechanisms to isolate
10. Resilience / continuity	Wireless backup for critical wired systems	Dedicated private cellular for failover or temporary installation
11. Governance/ compliance	Cameras for security, safety and documentation oversight	Private 4G/5G for site-wide throughput and flexibility
12. Innovation / new offers	"In a box" systems including wireless connectivity	Pre-integrated industrial or commercial systems including P4G / P5G connectivity
13. Skills & staff	Worker safety monitoring	Connected work-wear, cameras, proximity sensors etc
	AR/VR training & assistance for field-workers	Indoor / outdoor reach + low & reliable latency
14. Customer experience & satisfaction	Improved indoor wireless access and reliability	Neutral host support, or issuance of venue SIM/eSIMs

© Copyright 2023 Celona Inc. All rights reserved.

Top 3 Use Cases for Private Wireless

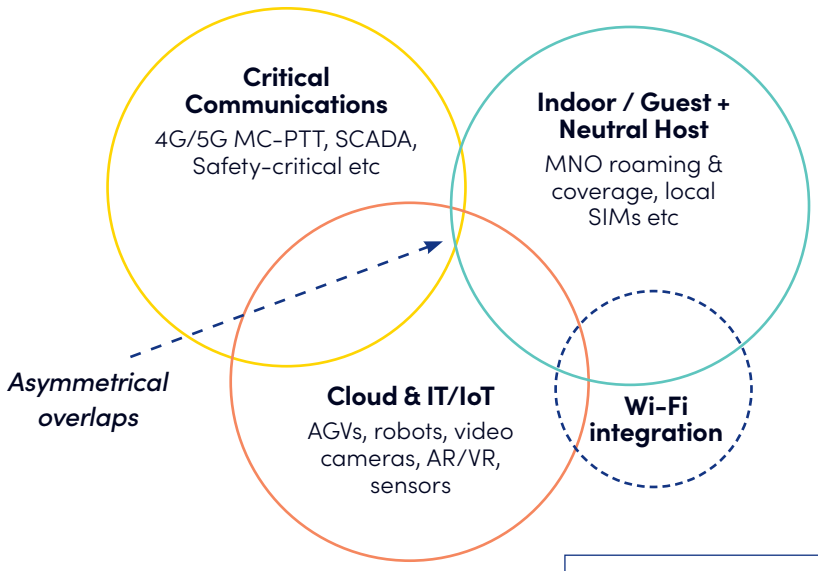
Many new applications require wireless connectivity. Reliability, security, ease-of-deployment and simple operation are key. Individual localised applications may generate positive ROI on their own, but complete site-wide or multi-site networks can expand the impact and value. Such infrastructure can be run by the enterprise itself, various types of service provider, or embedded into larger systems.

There are many options for connectivity, which vary in capability, cost and flexibility. Today enterprises rely on wired ethernet, Wi-Fi, private radio and a variety of specialist industrial networks. They also use public mobile networks run by telecom operators/carriers (MNOs) for employee smartphones and wide-area assets such as vehicles.

Private wireless can be a game-changer. CIOs should view the opportunity through the lens of three very different primary functions for private 4G/5G, plus some smaller ones:

1. **Critical communications networks**
2. **Cloud and IT/IoT networks**
3. **Indoor mobile phone networks, including "neutral host" models**

Private 4G / 5G networks segments (2023/24+)



Also: campus & local-area fixed wireless access using private 5G

© Copyright 2023 Celona Inc. All rights reserved.

Critical communications networks

Critical communications networks made up the bulk of major private network deployments until 2022 and still remain very important.

They are typically deployed for utilities, oil & gas, mining, public safety, airports and military purposes. Often, they are used in rugged environments, for human communications (typically push-to-talk), in-vehicle gateways and specific automation systems such as remote sensors and monitoring systems.

Usually, they replace alternatives such as private mobile radio (PMR), TETRA and microwave fixed-links, often in locations that lack public cellular coverage. They have typically been packaged and deployed by specialist integrators for sectors like oil-rigs or field-deployment by military units. They vary widely in size, from a single portable network for public safety, up to a national network for a utility company.

There is little need for interconnection with public mobile networks; indeed it may be specifically avoided in order to maintain isolation for optimal security and "air-gapping" for critical applications. However, many users of critical private wireless subsequently look at additional general-purpose enterprise use-cases and applications, which may fall into the more general category of IT/IoT considered below.

© Copyright 2023 Celona Inc. All rights reserved.

Cloud and IT/IoT networks

This category of private cellular is receiving the greatest attention at present, and is growing the fastest.

It ties in with many parallel trends around cloud and edge-computing, AI and machine vision in factories, robots and AGVs in warehouses , security cameras and general IoT / smart building use-cases. It aligns with "transformation" projects in IT, plus some parts of the OT (operational technology) space such as smart manufacturing.

It tends to be viewed as a complement – or alternative – to other IT-type network technologies like Wi-Fi and fibre/copper ethernet. Given that many use-cases have a heavy cloud emphasis, there is more acceptance of virtualisation of cores and perhaps in future new RAN (radio network) paradigms such as Open RAN. That said, in the short to medium term most private wireless will use integrated architectures, rather than adding the complexity of multiple vendors and integration of discrete components.

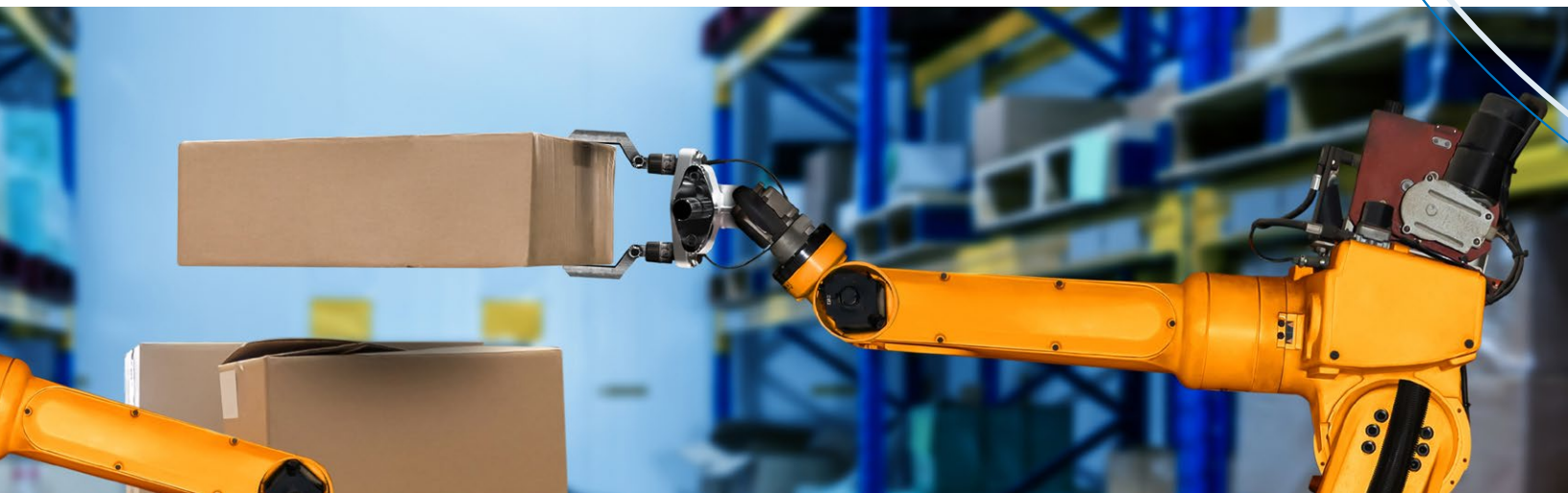
This is currently the area with the greatest amounts of innovation – although large-scale operational deployments are still comparatively rare (in the range of low 1000s globally). Recently there has been more focus on 5G than 4G, although that varies depending on the specific practicalities and economics. These deployments can be indoor-only, or span a campus site such as a business park, university or major manufacturing plant.

There is a growing focus on automation, replicability and ease-of-use, to drive down costs, enable a broader set of channels and delivery partners, as well as simplify skills and support requirements. This sector is stereotyped by the view that "private 5G should be as easy as Wi-Fi". In reality, there still remains more complexity, although the gap is narrowing – and it may by the greater role of managed services.

There are two sub-categories:

- **IT-type scenarios**, where private cellular can be seen as a sort of enterprise Wi-Fi-on-steroids vision, with terms such as "5G LAN" gaining prominence and mindshare. There is a small overlap with the coverage / neutral-host sector (see below), which may grow deeper in future.
- **OT deployments** in which private 4G/5G gets embedded into larger industrial automation or other systems, such as factory robots or dockside cranes. Companies like Siemens are integrating cellular into their portfolios, just as they have historically used WLAN and fibre. There is some overlap with critical comms.

Although the main focus for this model is in-building / campus networks, it may also extend to larger domains such as smart cities, as well as multi-location users such as retail chains.



Indoor mobile phone networks

Celona Neutral Host

In additional to enterprise connectivity for staff, IoT devices and vehicles, CIOs should also consider the need for normal public mobile network access at their corporate sites as a priority, especially for guests and visitors.

Private wireless is starting to support improved public cellular access, particularly via an approach known as "neutral host".

About 80% of ordinary mobile phone use is indoors – at home, in the workplace, or in visited buildings and venues. Often, coverage and performance is worse compared to outdoor settings, because of signal losses through brick, concrete and glass. This blocking effect gets worse at higher frequencies, such as those commonly used for public 5G. Many enterprise sites are in locations with poor outdoor coverage, such as in industrial zones.

Today, most in-building access to public MNO networks is delivered from outdoor cell coverage going through the walls or windows, or with some form of special indoor system. Historically, various types have been deployed, from simple "off-air repeaters" to very expensive DAS (distributed antenna systems) fed by carrier-installed radio equipment, effectively turning them into separate cells. The latter are mostly used only at the most important sites, such as sports stadiums, convention centres and airport terminals.

Various initiatives are underway to improve cellular coverage in mid-size buildings more economically, ideally with simpler MNO contracting. A central concept is the idea of the Neutral Host, which is an organisation providing indoor coverage as-a-service, acting as an intermediary between the venue-owner and one or more mobile providers.

One approach is to use a private 4G/5G network as the basis for neutral host services. The local network acts as an extension of the MNO's own coverage, using an interconnection to allow visiting subscribers' smartphones to (effectively) roam onto the dedicated indoor system.

There are various commercial models, which can involve property owner, tenants or MNOs paying, depending on the specific site and requirements.

At the moment this approach is growing fastest in the US, using CBRS spectrum for private wireless. In some other countries such as the UK, Germany and Switzerland there can be regulatory restrictions on using private networks for public MNO services, although these may change in future. Other approaches and architectures are becoming more important, such as the UK's MNO-agreed standard called JOTS Neutral Host.

Watch our webinar to find out more about Neutral Host.
celona.io/neutral-host/webcast

CIOs should be aware that neutral host is an important but early-stage innovation in private wireless. The exact delivery models and acceptance by major MNOs will evolve over the next few years.

In some cases NH capability will be a secondary application added to existing private wireless, while in others "NH-primary" deployments for mobile coverage may host the enterprise's dedicated wireless as an extra tenant.

© Copyright 2023 Celona Inc. All rights reserved.

Additonal use cases

Apart from the three primary enterprise areas for private 4G and 5G, some CIOs might also employ the technology for purposes like:

Community networks, especially in villages or rural/remote areas, where there is a lack of good public network coverage. It can also be used to backhaul outdoor public Wi-Fi.

4G/5G-based fixed wireless access, either for connecting remote buildings / structures for large enterprise campuses, or for municipal access to sites such as schools and hospitals.

Offshore and littoral connectivity,
for ships, ferries, windfarms and buoys.

Private networks for smaller sites, especially chains in retail and hospitality sectors.

© Copyright 2023 Celona Inc. All rights reserved.

Private wireless drivers, enablers and challenges

What are the top 5 drivers CIO's need to consider?

Coverage

A core reason for private 4G/5G is the limitations of network coverage.

- Public MNOs tend to deploy their network assets in areas with high population density, or along main roads. They rarely prioritise 5G rollouts for industrial zones such as ports and process plants, or in remote and rural areas. Indoor coverage is patchy, especially for buildings such as factories such as factories and warehouses with few "general public" visitors.
- Wi-Fi coverage tends to be short-range and predominantly in-building. It struggles to deal with industrial campus sites such as airport ramps or quarries, especially where vehicles need full connectivity. Lower permitted power levels mean sites with extensive metalwork or interior walls require a dense grid of access points and backhaul fibre.

Control

- Owning, specifying and/or operating private wireless allows companies to optimise many network parameters themselves, taking direct responsibility for security, reliability, performance and reporting. They may want to limit operational or personnel data transmitted outside their own IT domain, or customise mechanisms for identity, redundancy and cybersecurity. Private wireless also allows the wireless domain to be optimised for demanding applications like high-definition video uplink or low-latency remote-control of machinery. Some companies may also prefer to use more predictable licensed / shared spectrum rather than rely on the unlicensed bands used for Wi-Fi.

Cost

- Private 4G / 5G networks have multiple cost tiers and business models. They may save direct costs compared to alternative network technologies such as private radio (or public 4G/5G MNO services), or may be elements in a more complex calculation of "total cost of ownership". For instance, field networks capable of supporting AR headsets may reduce travel by experts visiting enterprise sites and also reduce downtime or workflow delays.

Cloud integration

- Historically, private cellular networks evolved separately from cloud technologies. Recently, maturing of both domains means there is a growing link between private wireless, enterprise cloud and hyperscale platforms. Networks are becoming more software-based and cloud-delivered, while cloud-based applications (such as IoT control, AI/analytics or digital twins) are more dependent on reliable local wireless and edge-compute.

Compensation (or monetisation)

- Some private wireless networks act as niche service-providers, rather than purely for internal enterprise connectivity. Site owners can act as "micro-MNOs" for 3rd party tenants onsite. For instance, an airport's private network may provide (paid) services to catering, maintenance and fuel companies' vehicles and personnel. Neutral host networks may allow property owners to charge higher rents to tenants, or benefit from "offload" payments from domestic or foreign roaming MNOs or MVNOs. Some enterprises may also become embedprivate wireless into solutions sold to their own customers.

© Copyright 2023 Celona Inc. All rights reserved.

Here are the important trends enabling private wireless in the enterprise:

Spectrum

- Historically, spectrum suitable for cellular (2G - 5G) wireless has been available only at a national or regional level, via auctions or allocations to telecom operators. In recent years many national regulators have started to allow applications for local spectrum licenses for a site or small area suitable for private networks, or have adopted dynamic sharing between multiple users. The US CBRS band is the best known, but others such as Germany's Campus licenses, the UK's Shared and Local Access licenses, and Japan's Local 5G are other examples. Although frequency band, rules and procedures differ, most developed countries now have (or are planning) some suitable spectrum options.

Equipment

- Until recently, most cellular equipment was designed for MNO "macro" cell towers for roadside or rooftop deployment. There are now more enterprise-grade small cells, including indoor variants. Unlike earlier picocells and femtocells, they are not dependent on integrating with MNO core networks.

Software and cloud

- The software elements of a cellular network – especially the mobile core – have been simplified and virtualised. They are now consumable by relative non-experts. Enterprises are in control of aspects such as security, identity, performance monitoring and reporting, creating user-groups and defining quality of service (QoS) needs. A range of SaaS models have also emerged in tandem, sometimes incorporating radio elements provided on an Opex-only basis.

Devices

- There is a growing range of suitable devices which can fully support private networks, including smartphones, industrial handhelds, cameras, gateways and various modules for IoT and vehicular use. These include support for suitable spectrum bands, as well as optimised OS support for "non-MNO" scenarios. However, there is limited choice where countries use unusual frequencies.

Ecosystem

- There has been huge growth in the number of integrators, application suppliers, vendors and consultants for private wireless. Industry associations such as OnGo Alliance (for US CBRS) or EUWENA in Europe provide documentation, certification and lobbying functions.

Tools

- There is a growing range of design, planning, monitoring, security and testing products and services for private networks available.

SIM and eSIM

- Historically it was difficult for enterprises to obtain SIM cards in low volumes, customised for private networks. The growth of the market has enabled much greater flexibility and understanding by key suppliers. Downloadable eSIMs point to even greater simplicity in future, perhaps by just scanning a QR code.

© Copyright 2023 Celona Inc. All rights reserved.

What challenges do CIOs face when implementing a private wireless network?

International Spectrum and Regulatory Variability

- International variability, especially in spectrum availability and regulatory rules for building and operating private cellular networks.

Scarce and Costly Skills

- Skills are still relatively rare and expensive. Most enterprises do not have private cellular technology specialists on-staff, especially with experience of deploying and operating core networks, 5G radios, SIM / eSIM and licensed spectrum.

Device Compatibility and Costs

- There may be a limited range devices or modules supporting a given version of 5G, specific spectrum bands and with software / OS control that fits with enterprise needs.

Integration with Legacy Technologies

- Integration with some legacy connectivity technologies and IT/OT systems may be challenging, especially if there is a phased rollout, rather than a full cutover.

Phased Deployment Alignment

- 5G technology is arriving in phases (or "releases"), with each generation including extra features. Enterprises may have to align use-cases with standards timelines.

Single-Site Deployments vs. Future Roaming Needs

- Most private wireless today is deployed at single sites. Future use-cases may require some form of roaming onto national networks, or across multiple sites.

Concerns of Vendor Lock-In and Interoperability

- Lock-in is a concern with new innovations – either relating to vendor choices and platforms, integration partners and service providers, or to the technology as a whole. Maturity will mean greater focus on interoperability in future.

This is an abbreviated description of key reasons private wireless is maturing, to the extent that it is now relevant to C-level executives. Details of specific technology or regulatory trends can be provided by Celona representatives or Disruptive Analysis.

© Copyright 2023 Celona Inc. All rights reserved.

Delivery, architectural and deployment models

Private wireless is designed for multiple use-cases and site types. The range of delivery models, as well as planning and deployment channels, is also broad.

CIOs should look for suitable templates and case-studies, and adapt them for their own company's specific locations and applications.

They should also engage with existing solutions providers, systems integrators and telecom operators that understand their business, as well as new supplier options that are specifically focused on private wireless. The last section of this paper covers decision criteria for selecting partners and vendors.

For private networks mostly used for critical communications, a wholly dedicated network may be appropriate. But for most IT/cloud-related systems there is much greater justification for integrating the 4G/5G elements with the main enterprise network and Wi-Fi domain. In some cases it may make sense to define user groups, or dedicate network partitions (or "slices") for specific applications, with different security or QoS parameters.

A private 5G network for a newly-constructed warehouse will have a different deployment pathway from one used at a mine, or for TV broadcasters at a major event. A retail chain with numerous stores will need different types of partners involved, compared to a nuclear power station, while a rural fixed-wireless provider might install its own local 5G infrastructure.

Most enterprises lack existing internal skillsets for operating private wireless infrastructure, so will typically require partners to offer ongoing support and evolution. Unlike Wi-Fi, there is a relatively small pool of trained engineers, especially with the knowledge to work across multiple brands of 4G/5G equipment and software.

Key delivery models for private wireless, and channels for obtaining them include:

In-a-box

- Self-contained solutions suitable for remote locations or harsh environments with limited cloud connectivity.

Integrated plug-and-play

- Options from a single vendor, which can be either on-premises or cloud-based, often with a portfolio of pre-tested applications and partner solutions.

General IT systems integrators

- Increasingly important as delivery channels for private wireless. Typically, these companies will be tasked with overall application or business-system design. As part of this, they may recommend or directly provide private wireless systems.

Telecom operators

Are obvious partners for private wireless in a number of situations. 5G has often been promoted as a platform for MNOs to offer high-value connectivity services to enterprises. Some initially struggled to deal with the customisation requirements and delivery models, but this is now changing with multiple telco pathways for enterprises:

- Systems integration units: Some operators have solutions units that provide IoT services, global data networks, consultancy projects and other offers. Some now offer private 4G / 5G campus networks.
- Vertical business units: Some telcos have business groups targeted at specific industry verticals. For instance, Telstra (Australia) has targeted mining, Telus (Canada) has a healthcare practice, Elisa (Finland) has a manufacturing arm. Such units are well-suited to adding private wireless.
- Network slicing: As 5G standalone networks roll out, MNOs are pushing slicing to carve out partitions for particular companies, sites or applications. Some early examples have been in domains such as broadcast networks.
- Hybrid networks: Combined public and private networks can enable onsite / offsite continuous coverage for vehicles and logistics, or separate connections for public devices.
- Major projects: Some telcos are involved in dedicated 4G/5G networks for national infrastructure projects, in sectors such as rail, military, public safety and energy. These may have dedicated spectrum and special equipment.
- Spectrum leasing: Some countries' regulators are mandating MNOs to sub-license spectrum on request, rather than offer dedicated spectrum bands.

Industrial system and vertical-specific integration providers

- May include private wireless in their own portfolios. For instance, specialists in industrial automation, mining, transport systems or critical communications may incorporate 5G hardware, software and devices as part of broader portfolios.

© Copyright 2023 Celona Inc. All rights reserved.

In-building specialists

- The rise of private wireless to support neutral host models is adding another set of delivery options – companies such as towercos or in-building coverage specialists, which have traditionally installed DAS systems are now also becoming important players for private 4G/5G as well.

Cloud Companies

- Are increasingly offering private wireless solutions on an as-a-service basis. This covers both partner and own-branded offers, sometimes bundled with additional capabilities for edge-compute, IoT and AI platforms. As private wireless evolves to more mass-market audiences and applications, the role of hyperscalers and smaller niche cloud specialists can be expected to grow

Managed service providers

- A range of MSPs are offering private wireless as a service for enterprises, either linked to existing connectivity offers such as SD-WAN and managed Wi-Fi, or within specific applications such as managed site security and surveillance.

WI-FI Specialists

- There is growing interest among Wi-Fi integrators, channel and individual engineers about private wireless. As propositions become simpler and more templated, there will likely be strong synergies.

Property and construction companies

- In some situations such as new-build sites, private wireless and neutral host deployments may be built-into the underlying fabric of new construction. This may enable different financing models, as well as allowing the firms to increase rental charges to tenants.

Overall, the private 4G/5G network world is now looking much more like the IT industry today. It has heterogeneous delivery models, many strategic and tactical partnerships, "co-opetition", integrators, consultants and sub-contractors, white-label business models, cloud-delivered "as a service" propositions and a far broader array of services providers.

© Copyright 2023 Celona Inc. All rights reserved.

The implementation process and ongoing management

Steps that CIOs should view as common across most deployments:

Planning and design

- Assessing the required network coverage, capacity, and performance needs of the application(s) and sites. This may involve physical on-site surveys and use of relevant planning tools, for both outdoor and indoor areas. Spectrum availability and regulatory constraints such as permissible height and power of radio equipment are also factors, as are the number and type of devices to be connected, required QoS characteristics, security and privacy architecture, and the integration with existing IT/OT systems.

Pre-deployment and preparation

- There may be preparatory work such as lab testing of a prototype networks, validation of solution design and administrative tasks such as application for spectrum licenses or other permits. There will be a need to set up physical locations for equipment, such as ensuring power supply, backhaul cabling or wireless links and cooling systems for servers.

Equipment installation

- This involves mounting, orienting and connecting the system elements such as small cells, edge servers, switches and routers. There may be regulatory requirements for registering the specific locations of the radios.

System configuration

- This involves ensuring the appropriate software, firmware, and parameters are loaded, and activating and registering the equipment with the network management system.

Network testing, optimisation and validation

- Various tests are conducted to check the network performance and functionality against the specification and design, such as signal strength, throughput, latency, coverage, interference, handover, and security. Any fine-tuning of network settings and parameters are conducted either by engineers or an automation function.

Device onboarding

- End-user devices will require SIMs or eSIMs, and to be registered onto the subscriber management part of the platform. This may be manual or automated, depending on the capabilities of the system.

Ongoing network management

- This involves monitoring and maintaining the network, with relevant software and hardware updates as needed. There may also be ongoing testing of live network security and performance ("service assurance").

Network and application evolution

- There should be periodic reviews of the network and its ability to support additional applications and use cases. It may be extended, perhaps from one building to a site-wide installation, or upgraded from 4G to 5G. A neutral-host capability may be added to a purely private network, or vice-versa.

Staff and skills development

- While initially enterprises may rely heavily on the expertise of integrators or managed service providers, over time they will likely wish to develop their own skills base, especially if private wireless becomes strategically important.

© Copyright 2023 Celona Inc. All rights reserved.

CIO decision-making considerations and criteria

CIOs must make a variety of choices when thinking about private wireless networks.

A few are partnership, tactical, and strategic in nature.

Strategic versus Tactical Approach

- CIOs must decide whether private wireless technology serves a tactical purpose to address specific problems at a site or if it's a strategic platform for multi-application use across multiple sites.

Partnerships, Integrators, Vendors, and In-House Development

- CIOs need to make decisions about partnerships, external integrators, vendors, managed service providers, and the development of in-house capabilities.

In addition, the following considerations cannot be overlooked.

Single-Vendor vs. Mix-and-Match Solutions

- The choice between using single-vendor systems or customized mix-and-match solutions needs to be determined.

Integration with IT, LAN, and OT Systems

- Decisions regarding the level of integration of private wireless systems with IT, LAN, and OT systems versus keeping them as separate overlay networks are crucial.

Impact on Business Case

- The integration decision will also influence the business case, with single applications offering easier ROI calculations, while general private network availability may yield greater financial and operational benefits in the long term.

Analogies with Ethernet and Wi-Fi Evolution

- Similar to the evolution of wired Ethernet and Wi-Fi, which began as single-application deployments and expanded to general-purpose networks, private wireless networks may follow a similar path.

Caution vs. Acceleration in Deployment

- Companies have historically taken a cautious approach with small lab trials and proofs-of-concept for private wireless. However, with more proof-points and case studies available, organizations are increasingly adopting private 4G/5G for specific point applications, aiming to expand usage over time. Horizontal expansion can be challenging if the initial deployment isn't future-proofed for broader use.

© Copyright 2023 Celona Inc. All rights reserved.

Strategic decisions

For a CIO, high-level decisions play a major role. Questions to consider include:

- Could private wireless eventually become strategic for the business, either as a platform for broader transformation, or embedded into its own products and services? Is there a vision or plausible scenario for this?
- How will private cellular integrate or coexist with other network technologies, given most will have their own evolution paths as well? Should it be loosely or tightly coupled in a common IT system? Will it have the same "cadence" of future upgrades, or does it risk being "out of phase"?
- How can an enterprise choose strategic partners with sufficient commitment, scale and resources to assist with multiple deployments and applications? (see below).
- Is 5G essential or is 4G sufficient for near-term applications? How does this align with spectrum, device availability, cost and other factors? 4G is lower-cost and more "productised" but 5G is future-proofed for future applications. Some countries' spectrum bands may be 5G-only. One solution is a dual-mode platform that can support either generation.
- What is the path toward repeatability of deployment? How can the enterprise benefit from the experience curve?
- What is a desirable level of inhouse competence in private cellular? What are the staffing and training implications?
- Are there any regulatory issues to watch? Some countries' rules limit the use of private networks for connecting public services, for instance via neutral host approaches. There may also be cybersecurity rules relating to particular vendors.
- Are external parties, such as major suppliers or contractors, aligned with the private wireless strategy? This may be important in sectors such as construction, or airports, where multiple companies operate in the same location.
- For international businesses, is it possible to align private wireless initiatives across the company? Are there local constraints in certain countries?

Most enterprises, except those with the most technically-capable in-house wireless engineers, will need deep partnerships for adopting and operating private cellular networks. There is now a broad choice of delivery options, as highlighted previously.

© Copyright 2023 Celona Inc. All rights reserved.

Tactical decisions

Considerations for a specific site/application:

- What are the specific needs being addressed? Is the primary driver related to network coverage, speeds & performance, security & reliability or other factors?
- Is the decision being driven by an internal project team, or recommended by a partner already engaged for higher-level system and process design?
- Is the implementation at a greenfield site, or retrofitted to existing networks?
- Are there any ROI "quick wins" involved, such as immediate payback from reducing costs of legacy systems, or improving process/workflow significantly?
- What is the status of private wireless usage elsewhere in the relevant country? Is suitable spectrum available and regulatory authorities supportive?
- How will private 4G / 5G integrate with, or replace, other connectivity technologies and broader IT system elements? While some private 5G solutions provide full visibility and integration with existing enterprise network and security policies, others offer an overlay network with limited visibility and managed by a 3rd party.
- Are suitable devices available for the application with 4G/5G connectivity in the available local spectrum bands? Are there any software / OS constraints?
- What resources are available for tasks such as network planning, design, security and ongoing operations / support? Can these be done in-house?
- How easily can a one-off initial deployment for a specific application be upgraded, extended or replicated in future?
- Which user groups will be involved? Employees, machines, IoT devices or visitors will have various non-technical requirements, such as privacy and ease-of-use.
- Relative benefits of a single-vendor solution (such as a central point of contact and the confidence of pre-integrated systems) vs. customised multi-vendor solutions, which offer more flexibility and less lock-in risk, but more complexity.

© Copyright 2023 Celona Inc. All rights reserved.

Partnership decisions

CIOs will be faced with complex partnership decisions, whether they deal directly with vendors or with their integration/delivery channels. Factors to consider include:

Experience and Use-Case Understanding

- Can they demonstrate relevant experience, as well as understanding of the specific customer use-case and vertical-sector business environment? Do they have application templates or blueprints available?

Trustworthiness and Reputation

- Trustworthiness and reputation: Are SLAs available, with references and metrics for previous support response-times and mean time-to-fix for problems?

Network Performance Compliance

- Can they conform to tight specifications for network performance, including downlink and uplink speeds, onsite network coverage and latency?

Commitment and Capabilities of the Partner

- How deeply is the partner involved with private wireless, and can they be expected to commit fully to it for years ahead? Do they have a strong internal team, diverse and flexible products, and their own industry engagement strategy?

Single-Vendor vs. Customized Solutions

- Do they offer single-vendor solutions proven to work effectively, versus a fully customised and integrated offer ("best of breed") that could align more specifically with requirements and need for inter-working with existing networks?

Support for IT and OT Applications

- Do they have the ability to support both IT and OT applications, including any current or future critical communications applications?

Capex and Opex Models, Customization

- Does the partner have both capex- and opex-driven models, and the ability to support customisation where required?

International Presence and Regulatory Expertise

- Can they operate internationally, with adequate staffing, local offices or delivery partners, and with relevant support for regulatory and spectrum situations?

Public-Access and Neutral-Host Potential

- Do they offer any scope for adding public-access / neutral-host ability in future? This may include relationships with MNOs / carriers, and regulatory/ security skills.

Multi-Technology System Flexibility

- Are they able to provide multi-technology systems that can blend private cellular with Wi-Fi, IoT networks or wired connectivity on a pragmatic and flexible basis?

SaaS vs. On-Premise Delivery Options

- Can they deliver both SaaS vs. on-premise options for private cellular?

Business Outcome Alignment

- Are they willing to specify and deliver against agreed business outcomes related to private wireless or the specific application it will be used for, such as productivity improvements, enhanced product quality or revenue uplift?

© Copyright 2023 Celona Inc. All rights reserved.

Conclusion

In conclusion, the evolution of private wireless networks, especially the widespread adoption of private 5G networks at enterprise sites, represents a pivotal strategic technology trend for CIOs.

From niche solutions in 2000, these networks have now become mainstream, driven by the availability of enterprise-suitable 5G equipment, software advancements, and the imperative for reliable and flexible wireless systems. With over 1000 large-scale private wireless systems already operational globally and the expectation of significant growth in the coming decade, CIOs find themselves at a critical juncture.

As these networks integrate with key technology trends such as cloud, AI, and cybersecurity, as well as sector-specific technologies like industrial automation and connected vehicles, CIOs must make informed decisions regarding partner selection, system integration, and connectivity to existing IT/OT systems.

This report underscores the direct correlation between CIO priorities and the maturation of private wireless technology, providing valuable insights into leveraging this transformative trend for strategic advantage in the digital landscape.

celona

celona.io

© Copyright 2023 Celona Inc. All rights reserved.

hello@celona.io

900 E Hamilton Ave Suite 200,
Campbell, CA 95008, United States

ABOUT CELONA

Based in Silicon Valley, Celona is a pioneer and leading innovator of enterprise private wireless solutions. The company is credited with developing the industry's first 5G LAN system, a turnkey 4G/5G system that enables enterprises and mobile network operators to address the growing demands for more deterministic wireless connectivity for critical business applications and vital use cases not met by conventional wireless alternatives. Celona's products and technology have been selected and deployed by a wide range of customers including Verizon, NTT, SBA Communications, Standard Steel, and Haslam Sports Group. To date, the company has raised $100 million in venture funding from Lightspeed Venture Partners, Norwest Venture Partners, NTT Ventures, Cervin Ventures, DigitalBridge and Qualcomm Ventures. For more information, please visit celona.io and follow Celona on Twitter @celonaio