TELECOM26 WHITE PAPER

Meeting the enterprise data security challenges of roaming on 4G LTE and 5G Private Networks

Private Networks are growing rapidly and are forecast to receive more investment than public networks over the next decade. But there are challenges around ensuring data security when devices roam between private and public networks.

Find out how Telecom26 overcomes these challenges to enable optimised and managed data security and integrity for mobile device access to Private Networks.

Introduction

Realising the potential of 5G Private Networks

The growth of Private Networks (PNs – also known as 'non-public networks' or NPNs) is not a new phenomenon, but LTE and, more recently, 5G technologies have drawn considerable attention to their potential, particularly in the manufacturing industry, as well as the transport and logistic sectors (such as airports). So much so that spending on 5G PNs is forecast to outstrip that on 5G public networks within the next decade.

Nokia's CEO Pekka Lundmark, recently commented that more money will be invested in private 5G networks than in public networks over the next 10 years

Low latency connectivity to drive 5G private network adoption

Polaris Market Research predicts that the global 5G private network market will grow at a CAGR of 40.9% between 2020 and 2028[1]. A rise in demand for ultra-reliable low latency connectivity for industrial applications, including industrial sensors and collaborative robots is a key factor driving the market growth, it says.

Meanwhile, ABI Research forecasts that the PN market could be worth US$16.3 billion by 2025. Furthermore, it predicts that spending on private and shared enterprise networks will surpass spending on public cellular networks within the next 15 years[2]. At the same time, while 5G is capturing the attention, 4G LTE is also expected to be widely used for enabling wireless connectivity. ABI Research also expects LTE to dominate this sector until 2028[3]. 5G is starting from a much lower base and, in any event, LTE is sufficient for many near-term use cases.

500+ companies currently investing in 5G private networks

But many in the industry believe that it will happen even sooner. Nokia's CEO Pekka Lundmark, for example, recently commented that more money will be invested in private 5G networks than in public networks over the next 10 years[4], particularly for use cases around mission-critical applications. Lundmark goes on to predict that every dollar invested in 5G private networks will return $4+ of end-user value.

...available data suggests that at least 500 companies have been, or are investing in, private mobile networks based on LTE or 5G as of December 2020. And this is likely to be a substantial underestimate of total global deployments .

5G PN deployments are growing rapidly. According to the GSA, "the exact number of existing private mobile network deployments is hard to determine, as details are not often made public", but it notes that available data suggests that at least 500 companies have been, or are investing in, private mobile networks based on LTE or 5G as of December 2020. And this is likely to be a substantial underestimate of total global deployments[5].

Of course, this represents an exciting opportunity for operators and providers alike, but for data security offers and information officers, the most important question is: "Will PNs ensure complete security and integrity for their corporate data?"

THE MAIN DRIVERS FOR PRIVATE NETWORKS...

DATA SECURITY
GROWING NEED FOR ENTERPRISE INFORMATION AND DATA SECURITY

LOWER TOTAL COST OF OWNERSHIP
ELIMINATION OF OTHER CONNECTIVITY (SUCH AS WIFI), AND REDUCED MOBILE SERVICE COST

5G
AVAILABILITY OF RELIABLE 5G SERVICES

SPECTRUM AVAILABILITY
BANDWIDTH FOR MASSIVE IoT AND M2M SERVICES

PERFORMANCE DEMANDS
NEED FOR LOW LATENCY, LOCAL PROCESSING FOR ULTRA-HIGH-PERFORMANCE APPS

CHANGING WORK PATTERNS
HIGH DATA CAPACITY, PRIVACY CRUCIAL FOR NEW EMPLOYEE NETWORKS

CBRS AND LTE-U
LICENCE-FREE SPECTRUM OPTIONS

Spectrum for enterprise Private Networks

Managing the availablity of spectrum

...traditional connectivity technologies...are unable to provide the reliability and availability required, nor can they offer the high-bandwidth, low-latency performance of 5G required for business-critical use cases...

Of course, 5G and LTE spectrum is generally licensed, so availability to enterprises may be subject to regulatory approval. However, unlicensed spectrum that offers similar performance characteristics is available. Citizens Broadband Radio Service (CBRS) which uses the 3.5 GHz band is authorised by the FCC in the US for wireless operations.

This is within the same range as mid-band spectrum for 5G, so offers significantly better performance than LTE – and, crucially, does not require spectrum licensing. Globally, Band N53 (2.4GHz) is also recognised by the ITU[6] and 3GPP[7] for mobile wireless connectivity, offering similar performance levels and a globally ubiquitous resource.

So, there are multiple carrier options, some licensed, some open – presenting a number of choices for the support of private network connectivity and to stimulate market adoption.

Drivers for the growth of enterprise Private Networks

Security and guaranteed performance

Increasingly, operators are offering PNs through network slicing, with each 'slice' dedicated to a specific PN, which theoretically should increase data security as each slice is dedicated to a campus or organisation.

A key commercial driver for private network deployments is Security. Enterprises demand visibility and control into all data traffic (specifically on mobile devices) in order to maintain overall corporate data security. A public/ macro network presents security vulnerabilities as it uses an unsecure and unmonitored encrypted IP connection that can be established within a restricted or secure area (private network), leaving corporate IP at risk.

A trusted network with guaranteed performance and security commitments that are beyond the capabilities of public mobile networks is required to ensure an overarching secure environment.

At the same time, traditional connectivity technologies, such as WiFi, are unable to provide the reliability and availability required, nor can they offer the high-bandwidth, low-latency performance of 5G required for business-critical use cases and applications.

The main drivers for Private Networks include:

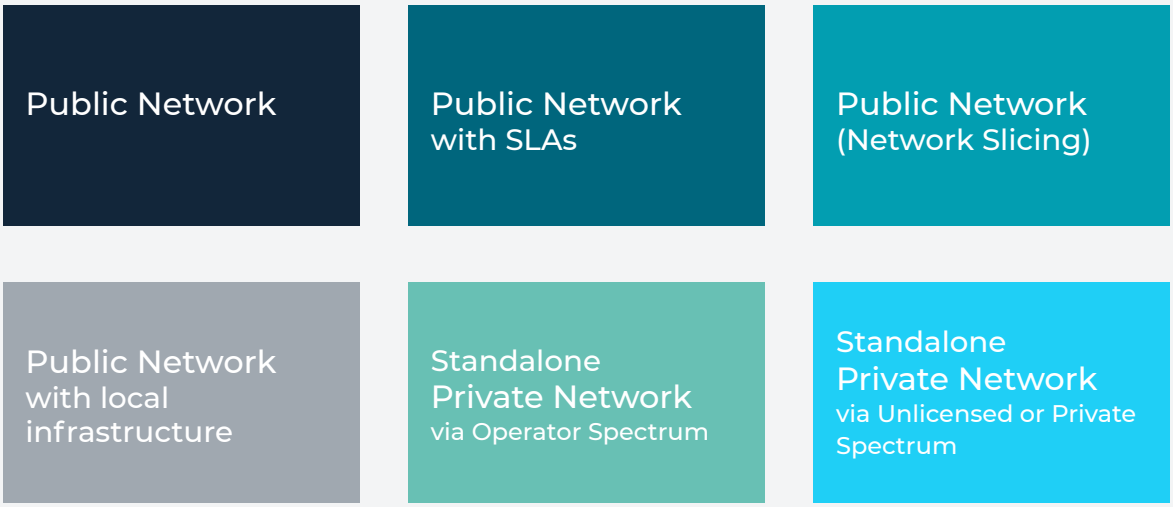
- Growing demand to ensure enterprise information and **data security**.
- **Reduced TCO** from elimination of fixed cable and other connectivity (such as WiFi), and reduced mobile service cost.
- The growth of **reliable 5G** services.
- Unlicensed/ shared spectrum **bandwidth availability** for massive IoT and M2M communications.
- Substantial **demand for low latency**, secure and affordable localised core private 5G networks, often associated with localised data processing capabilities for ultra-high-performance applications.
- **Changing work behaviour**, magnified by COVID-19, requiring higher data capacities and faster connectivity, as well as more secure private networks as employees and visitors move between private and public networks.
- Licence-free **spectrum options** such as CBRS or LTE-U.

Although some enterprises may consider deploying PNs using their own resources, operators can provide the know-how for deploying and operating such networks, or to assure a continuity of service between the islands of private networks.

Increasingly, operators are offering PNs through network slicing, with each 'slice' dedicated to a specific PN, which theoretically should increase data security as each slice is dedicated to a campus or organisation.

Increasingly, operators are offering PNs through network slicing, with each 'slice' dedicated to a specific PN, which theoretically should increase data security as each slice is dedicated to a campus or organisation.

Figure 1: The range of options for manufacturing/ production/ supply chain enterprises from Public Networks through to Private/ Dedicate Networks.



Source: GSMA

The diagram above shows the range of network deployment options open to enterprises today:

The problem is that most of these options still bring security vulnerabilities, and leave one essential issue unsolved: roaming between private and public networks.

The data security challenge of private-macro network roaming

Security and guaranteed performance

Private networks are not new, but the interface between private and public networks is (that is, roaming between private and macro networks), and this creates unique challenges for maintaining corporate security.

WHAT ARE THE SECURITY CHALLENGES?

DEVICE DATA TRANSFER

Devices on the network essentially act as a USB drive. Data can be transferred to and from devices undetected – by means such as NFC, USB, Airdrop, Bluetooth, and so on.

Once data is on the device, it can then be transferred on to the macro network / internet. Overcoming this challenge requires a means to visualise, manage and control data transfer on each device, and therefore prevent transferring the data.

MOVING BETWEEN PRIVATE NETWORKS

Employees need to travel into and out of PNs.

The only options to maintain this “walled PN security” are to either give employees two phones (one for the PN and one for the macro/public network), a dual-SIM, or to ban macro network-attached mobile devices from the PN altogether – no scenario is ideal.

DUAL-SIM PHONES

Using a dual-SIM phone (which uses one SIM for the macro network and one for PN) should theoretically overcome this challenge. However, this can still create issues:

- Corporate data that has been transferred to the device in the private network becomes visible once the device has moved into the public network – creating a security breach. But, as we will read later, T26 offers a unique solution to this problem.
- Handover between a PN and the macro public network can cause devices to 'drop out', with phones needing to reconnect to the public network – and vice versa – during the transition. In some cases, phones can go into 'idle' mode for up to 6 minutes.
- Handover is also hampered by the fact that the signal from a macro network is often stronger than that from a PN, and so the device connection preferentially connects to the public network, without any handover to the PN.

NETWORK SLICING

Network slicing – as offered by an increasing number of operators for PNs – means that data on a device is still exposed to the operator network.

More importantly, there is no visibility and control of the subscriber and data being transferred between networks.

All of these issues mean that data security is a key challenge, compounded by poor performance/user experience due to inadequate or absent network handover. How can data integrity be maintained, while enabling access to devices that can access both private and public networks, with the required handover performance?

Telecom26 provides a unique, reliable, and highly secure solution to overcome all of these challenges.

The Telecom26 Solution to Private/Macro Network Roaming

Secure, high-performance private network connectivity

Telecom26 has significant experience in providing optimally secure, high-performance PN connectivity both for greenfield sites and PN transformations and upgrades.

We work with our systems integrators (SI) and infrastructure affiliates and partners to provide an end-to-end PN deployment, or we can provide our unique Telecom26 SIM – either as single SIM, dual SIM, or eSIM hybrid – as well as advisory services to ensure the best data security possible.

Telecom26 solves the problems of private-public network roaming by not only ensuring controlled subscriber access, and reliable and rapid handover to improve QoE, but most importantly, ***Telecom26 enables complete visibility into all mobile data transferred to or from any Telecom26-enabled device on any network – public or private.***

When detecting a potential data security breach on a device, the Telecom26 solution provides a notification that allows Telecom26, in conjunction with corporate security policies, to view, manage and control that data transfer – thus eliminating any data security breaches. Telecom26 offers two options:

Our solution eliminates service disruption, while allowing Telecom26 and/or the enterprise to apply corporate security protocols to the device via Firewall or DPI.

1. Single Telecom26 SIM

If the private network is provided and managed by Telecom26 – and/or our SI and infrastructure affiliates and partners – our solution detects any query from the Telecom26 SIM when it wants to register to a known PN. Once the PN response is received, the SIM (device) de-registers from the macro/public network and registers on to the PN. Telecom26, therefore, makes the network handover and transition faster by controlling forced attachment via API control to the device.

The advantage of this approach is that it complies with the PN and macro standards – unlike apps – and Telecom26 (and the enterprise) can securely control the transition between the private and public network, ensuring that no data is exposed to the macro network. In addition, it offers the benefit of single billing.

However, it's important to note that if the PN is not provided by Telecom26 or our partners, the issue of delayed and/or absent handover is still present. In this case, Telecom26 offers a dual SIM solution, to solve that issue.

2. Dual Telecom26 SIM

Telecom26 provides a dual SIM for devices – either as dual physical SIMs, or as a physical and an eSIM. While one SIM is connected to the macro network, for example, the other SIM is searching for known PNs – and vice versa – according to network coverage and signal strength. The advantage is that, as both SIMs are Telecom26 managed, once one of the SIMs has connected to a PN, the other remaining SIM is de-registered from the macro network and disabled.

Working with our affiliates and partners, Telecom26 can provide an end-to-end solution for greenfield deployments – from network infrastructure deployment to managed security.

The same process occurs when the device moves from the PN to the public network – meaning that enterprise data is never exposed to the public network.

Our solution eliminates service disruption, while allowing Telecom26 and/or the enterprise to apply corporate security protocols to the device via Firewall or DPI. A further benefit is that a fully Telecom26-enabled device will send a notification of any security breach as the device moves between networks – as Telecom26 enables all services and transactions to be managed by the corporate customer in conjunction with their security policies.

The Telecom26 SIM provides optimum corporate data security whether for greenfield or existing PN deployments. The unique Telecom26 SIM – single or dual – offers security, reliability, performance, controlled access, roaming and scalability far beyond that offered by any macro network, or via network slicing.

In essence, our Telecom26 SIM solution 'locks down' the PN – only Telecom26 has the means to do this today.

Changing work behaviour, magnified by COVID-19, requiring higher data capacities and faster connectivity, as well as more secure private networks as employees and visitors move between private and public networks.

Greenfield vs. existing Private Network deployments

Working with our affiliates and partners, Telecom26 can provide an end-to-end solution for greenfield deployments – from network infrastructure deployment to managed security. For example, one of our partners is also a partner of Nokia, one of the leading exponents of PN deployments, helping the Finnish providers to deploy large-scale PNs.

For enterprises with an existing PN, meanwhile, Telecom26 provides Telecom26 SIMs and advisory services in order to configure and transform the PN to provide seamless mobile connectivity with managed subscriber control.

Put simply, Telecom26 can provide the entire end-to-end solution in conjunction with our affiliates and partners, including managed subscriber access and control, and we can work with other partners to provide our unique SIMs, as well as advisory services, ensuring optimal corporate data security.

Either way, we can meet the demanding requirements of 5G private networks across a range of use cases and sectors.

Conclusion

Secure, high-performance private network connectivity

Rapid deployment of 5G is accelerating demand for PNs in the enterprise sector, as 5G enables high-bandwidth, data-intense, low-latency applications on a localised core for a spectrum of industries and sectors.

PNs offer significantly tighter data security, reliability, availability, and are able to meet the often stringent performance demands of mission-critical applications.

They enable operators, service providers and SIs to offer multidimensional SLA guarantees to enterprises, including optimised radio coverage, guaranteed network performance, security and reliability for mission-critical use cases. However, roaming between private and public networks brings a new set of challenges around corporate data security.

We are the only provider that can offer secure roaming between public and private networks (with managed corporate security) through our dual Telecom26 SIM... all on a single bill.

Telecom26 can provide end-to-end greenfield PNs using our unique dual Telecom26 SIM that not only controls and manages which network (public or private) a device registers to, but also provides instant notification of any 'undetected' data breaches – which can occur on non-managed networks – as the device moves between the macro and private network.

Furthermore, our SIM ensures the best possible user experience in terms of handover between networks, with minimal 'dropout' compared to other solutions.

Telecom26 also works with existing PN providers and/or enterprises to transform their PN using Telecom26 SIM(s), combined with our experience of providing advisory services, to ensure the tightest data security and best QoE.

Whether you're an enterprise, SI, network infrastructure provider or service provider, Telecom26 has the solution to help you optimise corporate data security. ***We are the only provider that can offer secure roaming between public and private networks (with managed corporate security) through our dual Telecom26 SIM... all on a single bill.***

Contact us now to find out more.

Case Study

Telecom26 enables global SI to deliver managed mobile security for a leading chemicals manufacturer

A leading US-based producer of materials and chemicals experienced issues with data security and data leakage from one of its manufacturing facilities due to the use of employee mobile devices. It had two choices: ban all on-site mobile devices; or, deploy a private network with fully managed security capabilities.

Mobile devices can be viewed as 'USB-like storage devices', transferring data almost undetected via means such as NFC, USB, Airdrop, Bluetooth, and so on. Once on the device, this data is then visible to many other connections, including the Internet. Of course, this can create a security breach for organisations if a device is not fully security managed.

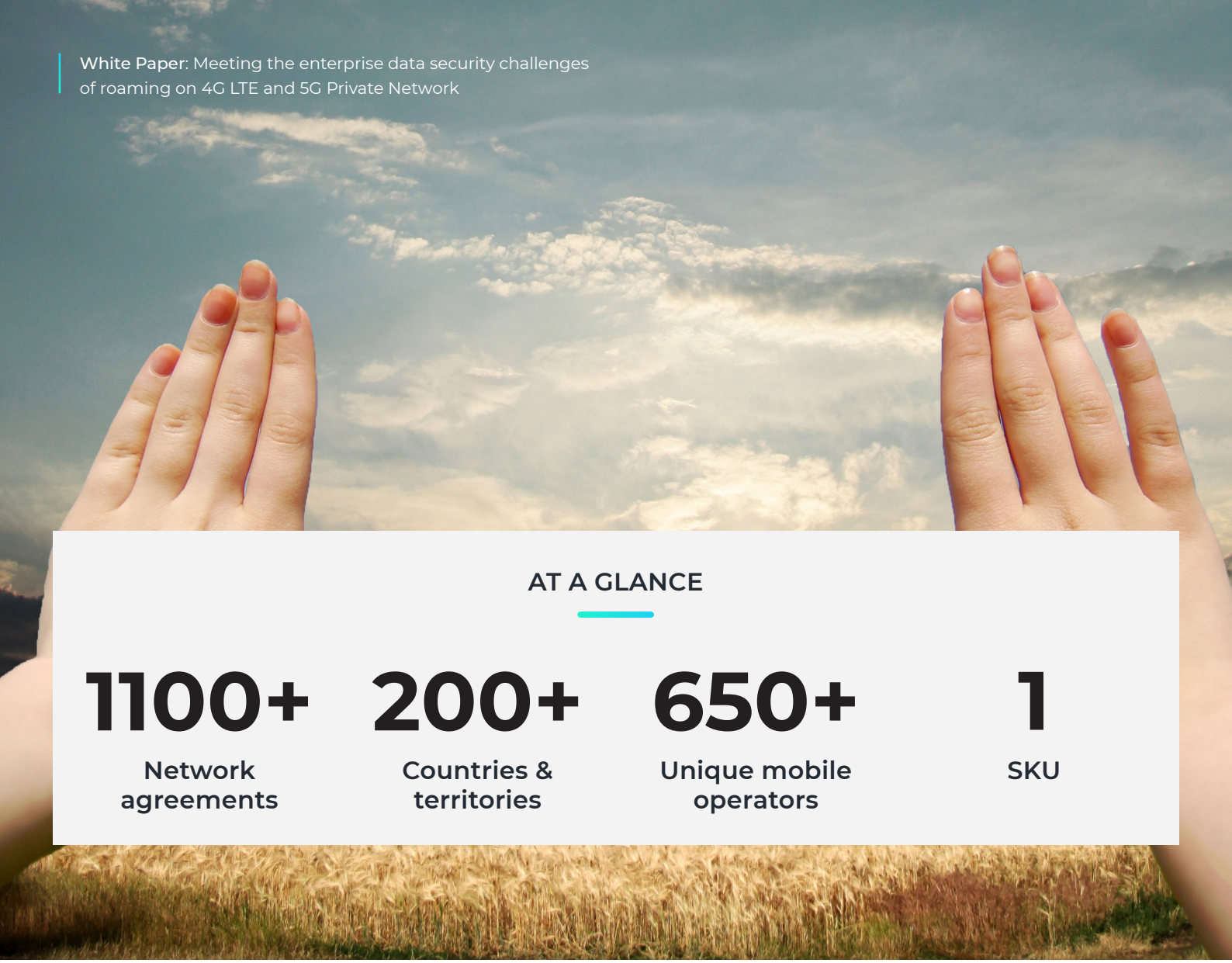
In this case, the customer chose one of the world's best-known systems integrators (SI) to deploy a greenfield private network. In turn, Telecom26 was chosen to work with the SI to provide complete security management for all mobile devices used on the customer site. The customer required 500 managed devices – however, the Telecom26 solution can scale limitlessly should the customer require expansion in future.

Put simply, Telecom26 can provide the entire end-to-end solution in conjunction with our affiliates and partners, including managed subscriber access and control, and we can work with other partners to provide our unique SIMs, as well as advisory services, ensuring optimal corporate data security.

Telecom26's unique dual-SIM solution now provides the customer with complete visibility into all data transferred to or from any Telecom26-enabled device, whether it's on the public network or the customer's private network.

If any data security breach is detected, the Telecom26 SIM sends a notification to the customer, allowing them to 'lock down' the device by ensuring that no sensitive data is transferred from the device.

A further benefit of Telecom26 dual SIMs is that they ensure managed connectivity of the device to the most appropriate network – so, if one SIM detects that the device has entered the private network it will ensure optimal connectivity, while the other SIM is de-registered from the public network – ensuring that data is never transferred unwittingly between the two. The same process occurs when the device leaves the private network.



AT A GLANCE

1100+
Network agreements

200+
Countries & territories

650+
Unique mobile operators

1
SKU

The dual SIMs also minimise device 'drop out' as it moves between private and macro networks, thus ensuring improved QoE for the user.

Telecom26 is unique in being able to offer a dual-SIM managed security solution for private networks. We work with major SIs (as in this case) to provide full mobile managed security, or we can also provide our own end-to-end solution through our network of infrastructure and connectivity affiliates and partners – one of which is currently helping Nokia to deploy private networks.

References

Footnotes and attributions

1. https://www.polarismarketresearch.com/industry-analysis/private-5g-network-market/request-for-sample

2. Malik Saadi, Vice President, Strategic Technologies at ABI Research, talking at the virtual ABI Research 5G Technology Summit in July 2020. https://go.abiresearch.com/lp-covid-19-impact-on-5g-deployments-and-boosting-global-gdp?utm_source=tech%20target&utm_medium=media

3. Cited in “Enterprise IoT Insights”, April 2021

4. https://www.electronicsweekly.com/news/business/private-network-5g-pending-outpace-public-network-spending-says-nokia-ceo-2021-02/

5. https://gsacom.com/paper/private-mobile-networks-december-2020-global-update/

6. https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/Events2019/Togo/5G-Ws/Ses1Joaquin_5G%20SpectrumRegulation.pdf

7. https://www.lightreading.com/5g/3gpp-approves-globalstars-spectrum-band-for-5g/d/d-id/758418

Telecom26

Telecom26 AG. Bahnhofstrasse 10, 6300-CH Zug, Switzerland
+41 43 500 42 44
www.telecom26.ch