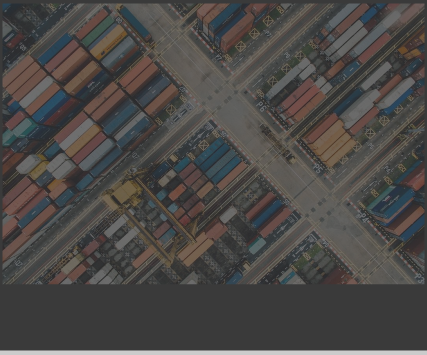
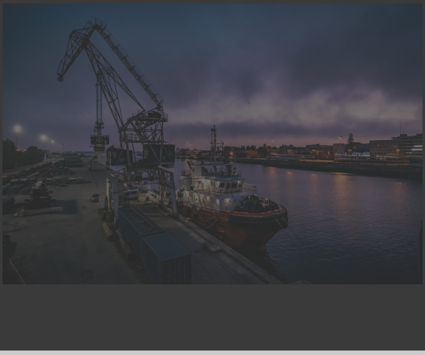
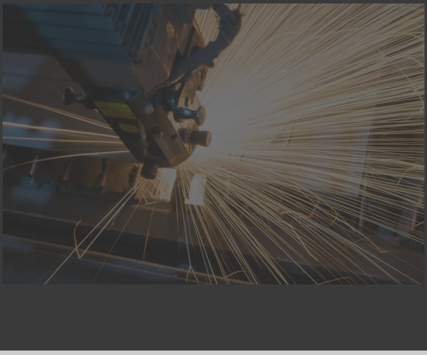
Connectivity Enablement for Private Networks

A Kaleido Intelligence whitepaper commissioned by BICS







bics

Kaleido Intelligence

Key Takeaways

Interest in Private LTE and 5G networks has grown dramatically over the past 3 years. Cellular networks offer a reliable, secure and highly flexible technology solution that enables businesses to improve upon and streamline existing business operations, as well as open the door to new types of activities.

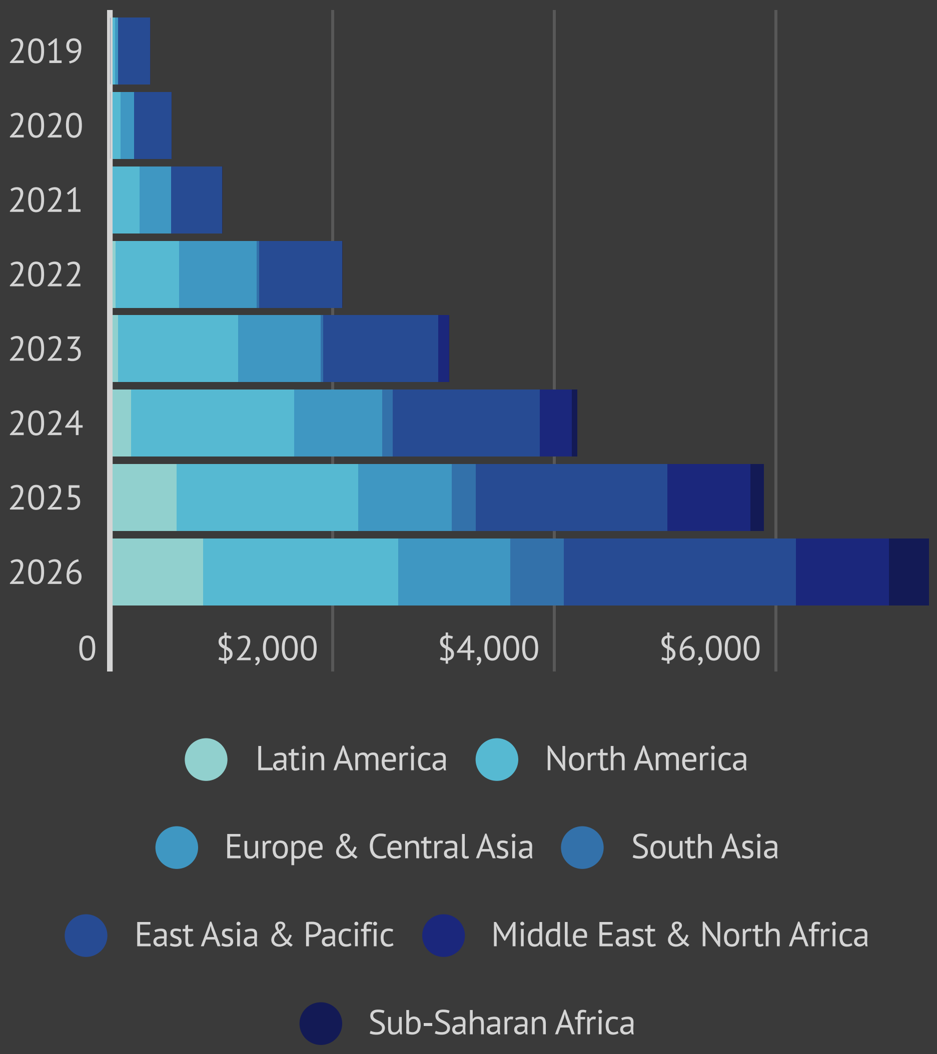
High bandwidth, comparable to wired Ethernet

High reliability & security, device-based authentication

Flexible & suited to almost any application

Avoids costly wired installations

Although the market is at a relatively early stage of development, growth is anticipated to be rapid. By 2026, over 22,000 sites globally are expected to use either Private LTE or 5G technology, with spending set to exceed $7 billion annually in 2026.

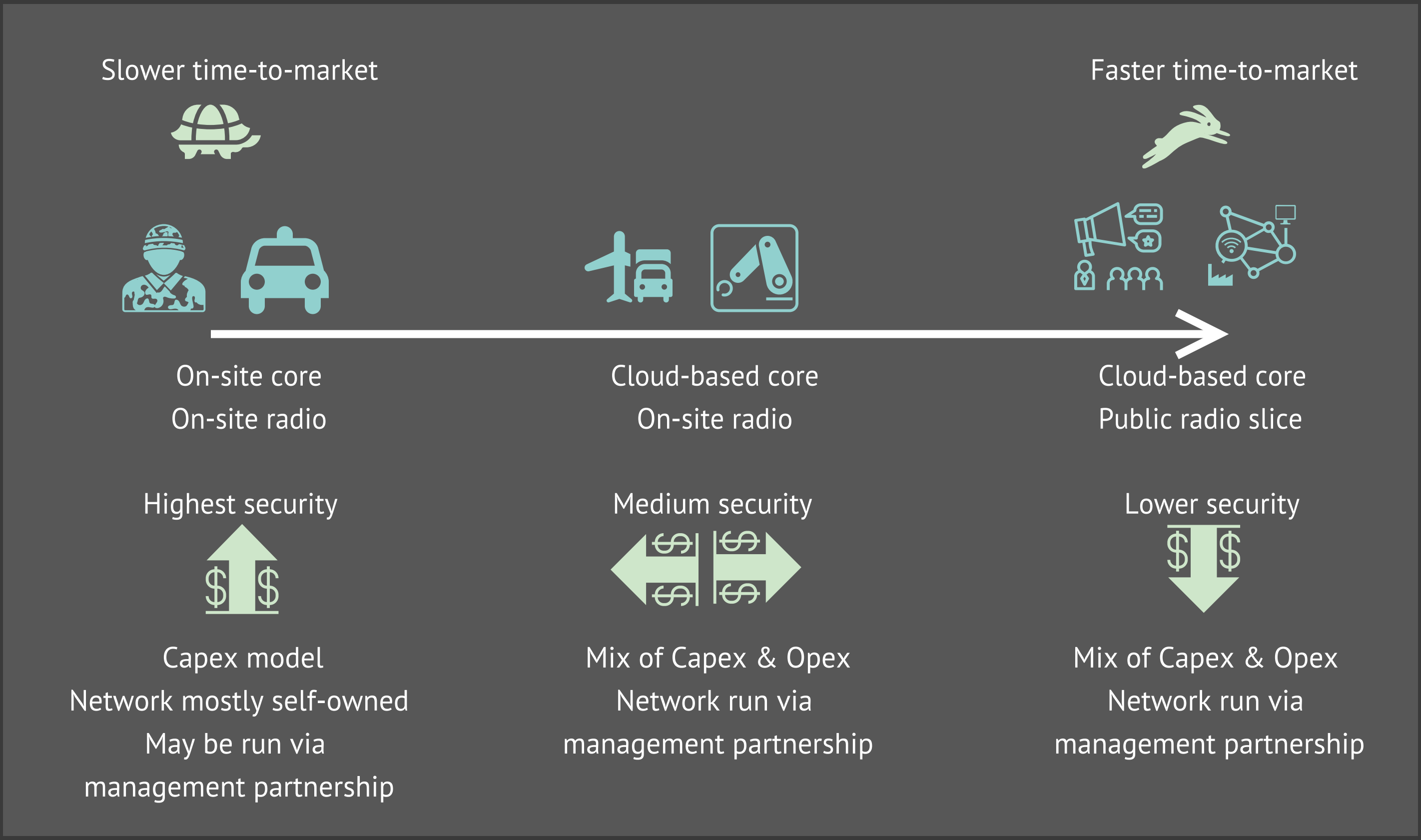


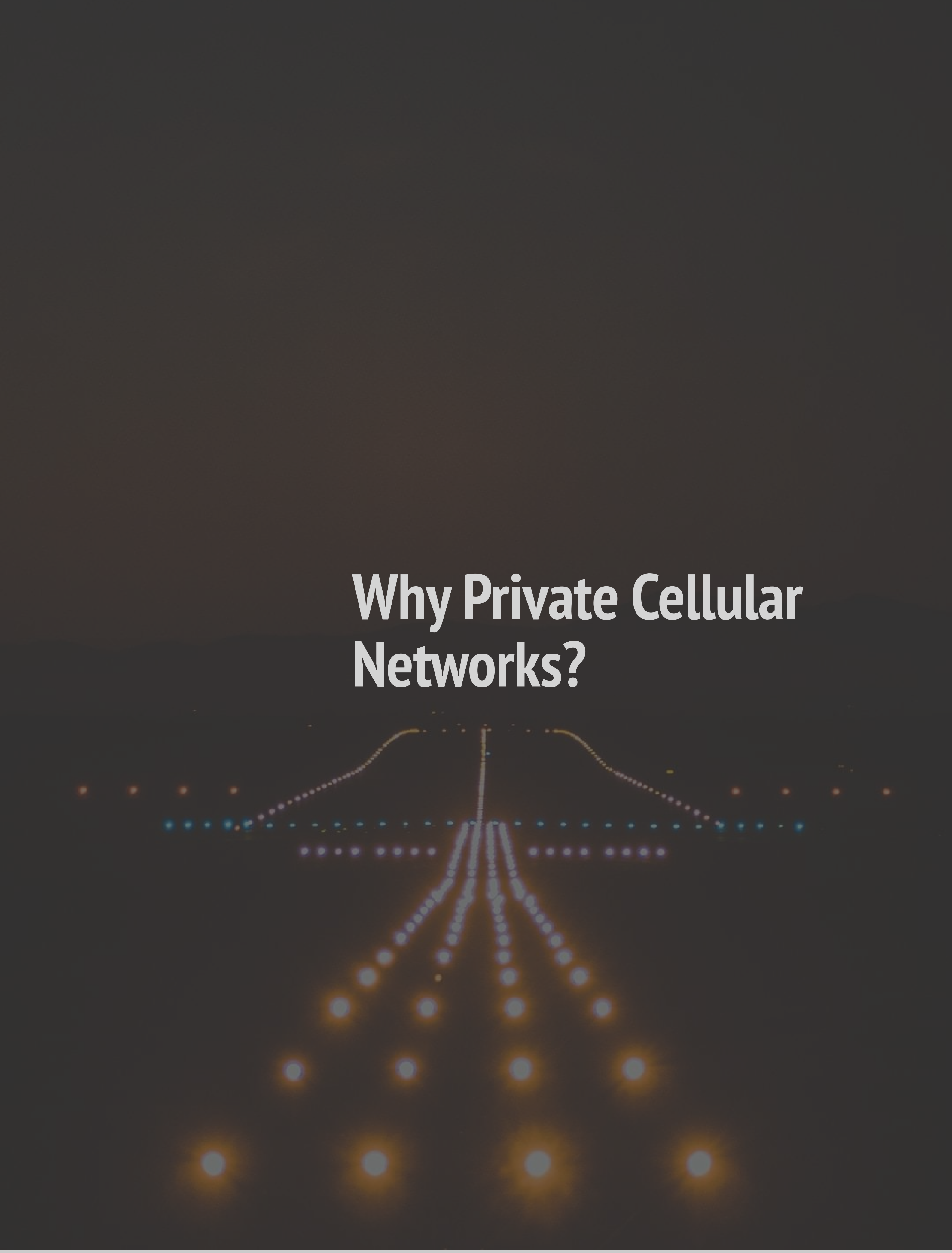
Historically, Private Networks have only required connectivity on-site, due to very high security requirements coupled with challenges in achieving seamless coverage across private and public mobile networks. However, there are many cases where this type of connectivity is desirable. For instance, products manufactured in one site, but operating in another may well require connectivity both at the point of manufacture as well as at the point of operation. Meanwhile, assets and devices operating in logistics and transportation hubs may need to access sensitive, private network restricted applications, while maintaining connectivity as they leave the site and travel to delivery points away from the Private Network site. The complexities of these types of setups are now being addressed by some players on the market in order to meet customer demand.

Military, government, public safety and critical operations use cases typically require the highest security and control over the Private Network. Inter-site connectivity and connectivity to the public mobile network is mostly undesirable.

Transport hubs and manufacturing facilities often require seamless connectivity between the Private Network site and the public mobile network as assets move in and out of the site.

Understanding and navigating the Private LTE and 5G market is no easy task, due to the fact that LTE and 5G technologies are not well understood from a deployment and management perspective in traditional enterprise settings. Enterprises must in the first instance understand the benefits of Private LTE or 5G against other, potentially lower cost technologies, while examining how that deployment should be managed from a connectivity perspective. In turn, this will aid in selecting the right partner to deliver an end-to-end connectivity solution.





Why Private Cellular Networks?

Private Network Advantages

Private Networks are not a new concept. Millions of sites across the globe have deployed Private Networks in the form of Ethernet, enterprise Wi-Fi, TETRA, DMR and MPT-1327 to support a variety of use cases ranging from emergency services, taxis, mining, oil and gas as well as commercial office communications. What has emerged over the last 3 years however, is rapid interest in Private LTE and 5G networks.

To a significant degree, demand for Private cellular networks has been driven by enterprise digital and IoT transformation strategies. Where traditional private networks have been deployed to establish a security and privacy for communications, emphasis is now on connecting assets, including machines, sensors and other objects to address use cases such as monitoring, automation and business analytics, with new services developed around these data streams. Here, Private LTE or 5G networks offer the high level of security and privacy expected of private networks, while also enabling real-time communications for data produced by the various networked elements. Where legacy technologies are often associated with compromises; Wi-Fi is subject to interference, while Ethernet is costly to install as well as being inflexible to changes for example; cellular technology does not suffer from these.

It is important to consider at this stage what Private LTE or 5G can achieve. Where businesses in the past may have used TETRA for communications or Wi-Fi for asset monitoring, cellular technology can address both of these use cases, and more, via a single solution, while also offering greater reliability and flexibility. When considering the future scope for business activities, where a range of use cases may be implemented, the ability to leverage a single technology standard and network comes with significant benefits and reduced complexity. Applications ranging from simple sensor monitoring to push-to-talk and high bandwidth video can be supported by LTE and 5G, meaning the technology can be used for a very broad range of use cases.

While LTE and 5G are undoubtedly low-compromise technologies for Private Networks, this is not the only reason behind the rapid rise in enterprise interest in using them. Across the globe, many countries have, or are in the process of releasing dedicated spectrum for enterprise Private LTE or 5G use. This means that a large number of specialist companies are now positioned to provide services for enterprise customers in a manner that most MNOs have simply not been able to in the past. Coupled with this, strategically-focused MNOs are increasingly open to working with a variety of industry players to enable Private Network deployments, either through a spectrum leasing model, or in some cases, by offering services further up the value chain.

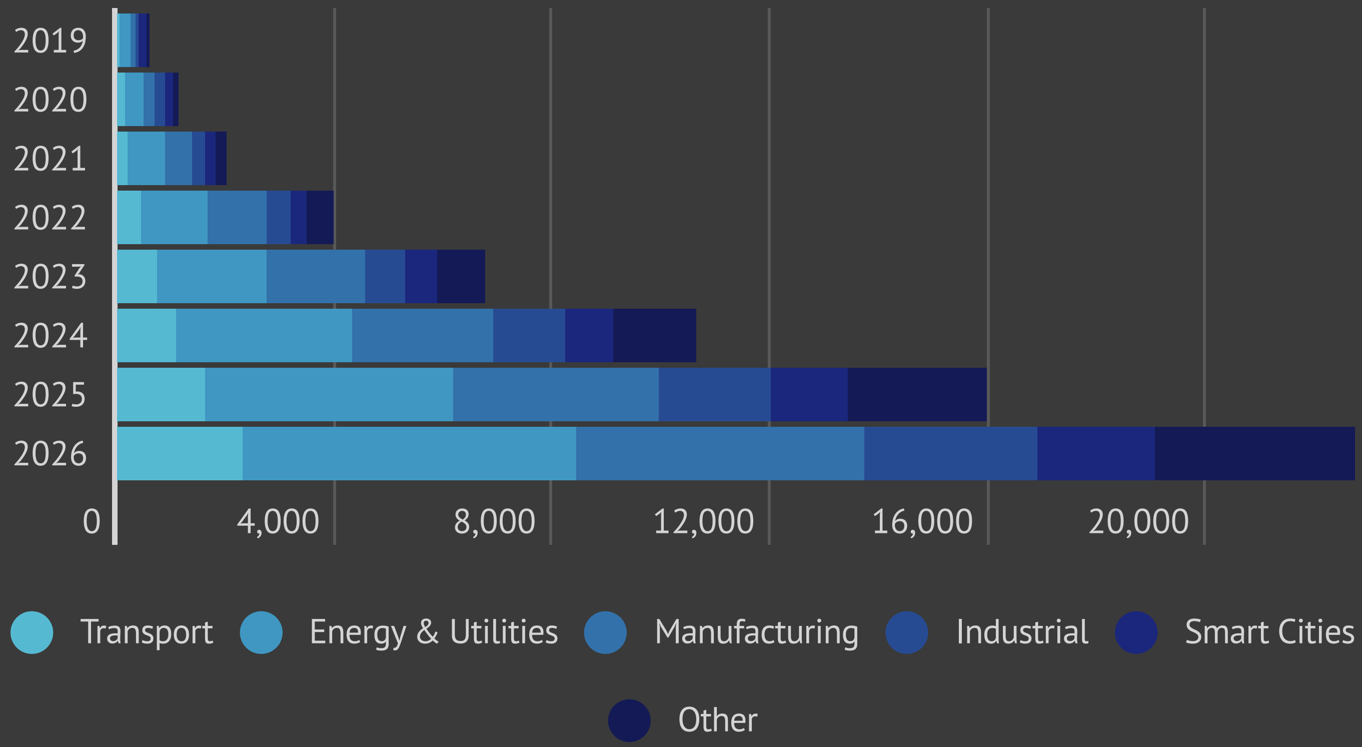
The emergence of the 5G standard brought significant hype with it in regards to network slicing. Network slicing offers the means to logically separate radio and core network functions from the public network, with the aim of addressing specific Quality of Service (QoS) requirements for slice customers. The virtualised, service-orientated architecture of 5G makes network slicing an ideal candidate for delivering a variety of specialised services to customers, ranging from international roaming to transport, manufacturing and others, such as utilities. Nevertheless, real-world commercial offerings for network slicing have barely even begun, with most 5G MNOs focused on maximising the potential for low-risk public 5G broadband adoption. Part of the reason behind this is the high level of complexity associated with network slicing in terms of orchestration, QoS monitoring and security. Many MNOs are simply not in a position to provide services at present. Additionally, broad consensus around business models has not been reached, which means that forecasting for expenses and monetisation is difficult. Furthermore, the way in which network slicing is designed within the 5G standard means that the intention is not to deploy a slice of the network for each individual customer. Therefore, core network and radio resources will be shared between customers with similar business needs. For example, automotive OEMs may use common functions and resources within a slice that has specifically been configured to manage automotive use cases. In many instances, this type of architecture will mean that the additional separation that is possible with Private Networks will be preferred, as it allows customers to receive a more customised service, while the dedicated nature of network functions will mean that security is enhanced.

The slow growth of network slicing has undoubtedly acted as another driver behind the interest in Private LTE and 5G networks: the potential to leverage dedicated portions of the public network for business operations has alerted many enterprises to the possibilities of using cellular technology for specialised operations. However, the touted model for providing this service has been slow to arrive. In turn, this has generated interest in cellular Private Networks.

In addition to the above, many enterprises and organisations have accelerated digitisation strategies as a result of the COVID-19 pandemic. IoT in particular is viewed as a mechanism for streamlining operations, automation and revenue assurance, where the pandemic and resulting restrictions imposed by governments across the globe have disrupted business-as-usual operations. The result is that cellular Private Networks are expected to benefit in several industry verticals.

According to Kaleido Intelligence, the base of LTE and 5G Private Network sites is projected to increase from 576 in 2019 to 22,719 in 2026, representing a CAGR of 69% during the time period. Europe, East Asia and North America are expected to account for the bulk of Private LTE and 5G deployments, with a substantial number of sites deployed across verticals such as energy and utilities (including oil, mining and gas projects), manufacturing and transportation.

Private Network Sites Split by Vertical 2019-2026



Current and Future Use Cases

Private LTE and 5G networks can be deployed under a variety of models, depending on the requirements of the use case and the customer. Historically, Private Networks have been configured as fully-isolated entities, with all data and communications confined within the secured zone. Naturally, such configurations are possible with LTE and 5G, but have normally involved a high capital expenditure for customers due to on-site core network hardware, radio units and UE in addition to costs involved in design, set up and other ancillary costs. Typically, these sites have been deployed for business-critical operations with very high security and performance requirements, with relatively little desire for inter-site connectivity or connectivity enablement for devices that operate both inside the Private Network as well as outside.

As the customer base for Private Networks expands, the dynamics in terms of connectivity requirements are changing. In the first instance, an increasing number of Private Network customers are interested in inter-site connectivity, whereby two disparate sites can be linked in order to share data. However, this desire is not always practical to implement due to the fragmented nature by which Private Networks can be deployed across the globe in terms of spectrum availability, partners and hardware support.

However, requirements are also changing in terms of how connectivity is enabled for individual sites; particularly for vertical industries such as transportation and manufacturing. In this context, the desire to support connectivity for devices both inside the Private Network as well as when those devices migrate outside of the security zone is increasing.

Case Study: Charles de Gaulle, Orly and Le Bourget airports

In July 2020, Groupe ADP (Aéroports de Paris) and Air France commissioned several service providers, including Ericsson and Athonet to deploy a cellular Private Network solution at the Paris Charles de Gaulle, Paris Orly and Paris Le Bourget airports, using LTE and 5G technologies.

The project is overseen by Group ADP's subsidiary Hub One, which owns a spectrum licence for cellular Private Networks. Once the project is completed by the end of 2021, the airports' 120,000 employees and contractors will be able to access a dedicated cellular network for professional services at the sites, across all public and reserved indoor and outdoor areas.

Additionally, services will not only be available to both Air France and non-Air France airlines, but also integrate operations across all 3 sites to boost collective operational efficiency.

Airports have traditionally relied on a combination of TETRA and Wi-Fi for site workers, which is often compromised by low bandwidth communications or patchy and unreliable Wi-Fi coverage. The LTE/5G solution will enable all workers' terminals as well as connected site assets to access a more reliable and higher throughput connection, resulting in improved efficiency and productivity.

While many of the endpoints connected to the Private Networks will remain on-site during their lifetime, the mobile nature of the workforce and certain airport assets means that providing connectivity both on- and off-site for devices that migrate in and out of the airports is an important feature of the solution. Meanwhile, the global nature of the aviation industry means that workers and connected objects are likely to be based in various countries around the world. In this context, it is thus important that international workers are able to access both public and private network services reliably in order to ensure optimum efficiency.

Case Study: Ford Electric Vehicle Manufacturing

In June 2020, automotive manufacturer Ford commissioned Vodafone Business, with partial funding from the UK government, to deploy a Private 5G solution at its E:PriME (Electrified Powertrain in Manufacturing Engineering) facility in Dunton, Essex. The aim of the project was to reduce delays in manufacturing, increase bandwidth across the campus, improve security and reliability, and increase productivity through real-time connected asset control, data analytics and remote support.

Ford noted that the 5G solution will replace its existing Wi-Fi network, which will enable both finer-grained security controls in addition to higher reliability throughput and lower latency.

These are critical features for factory operations, where connection density and data traffic levels are high, while high security is paramount to protect business operations and ensure the production of reliable and safe products.

In addition to the Dunton site, a second deployment was announced at welding specialist TWI's site in Cambridge, using 5G technology to provide the same benefits. In both instances, secure routing of traffic will be critical, due to the sites' intended use of remote worker expertise to support operations. This means that the data produced by sensors installed on welding robots and automated guided vehicles must remain securely within the Private Network, while video data used for support must be routed to remote workers securely.

As we have seen from the case studies above, emerging cellular Private Network solutions require a high degree of flexibility – most notably across specific verticals. These include:

- Airports
- Maritime ports
- Logistics warehouses
- Logistics fleets
- Manufacturing and industrial facilities

In all of the use cases above, Private Network customers often rely on a high degree of mobility in terms of the workforce as well as devices and assets used inside the Private Network. As we will observe in the following section, authenticating and seamlessly integrating devices that move between public and private networks is not a simple task, and requires the services of a specialist to ensure that service delivery is optimised.

An Enterprise Roadmap to Private Network Success

Private LTE and 5G deployments are challenging to implement, both from an enterprise customer perspective, as well as from a service provider perspective. This section will examine how enterprises should consider the market across several aspects.

Costs

Very high confidentiality, high security deployments invariably involve significant Capex investment in addition to management complexity, unless the customer's partner assumes this role. These types of deployments are typically fully on-premises, requiring all core network and radio hardware to reside on-site. In most instances, devices will only be able to authenticate with the Private Network, providing assurance that no data leakage takes place that could compromise the security model. Although this model has suited high-capital enterprises, military and government services and carriers, it is not conducive to accelerating the market where enterprises wish to deploy high security projects on an Opex basis. Indeed, the same may be true even in hybrid cloud deployment types. Kaleido has found that some Private Network providers are thus examining the potential for Private Networks-as-a-service, where typically:

- SIMs are provided by the service provider.
- Network set up, configuration and management is handled by the service provider.
- In some instances, Private Network providers are examining partnerships with RAN providers to incorporate into the solution package. This opens the opportunity to subsidise RAN Capex via a subscription model.

The bulk of the customer's initial outlay will thus be through the acquisition of compatible endpoint devices, such as ruggedised tablets, phones and so on.

Expertise

Very few enterprises have in-house expertise where design and management of 3GPP networks are concerned. This barrier is overcome either by recruiting expertise into the organisation, or outsourcing the design and management expertise to a service provider. The ecosystem presently incorporates a large number of entities than can address these needs to varying degrees.

Compared to Wi-Fi or wired LAN networking, LTE and 5G management requires in-depth knowledge to ensure that security, QoS, subscriber access, signalling, API configuration and so on are set up and monitored correctly. Some vendors, have developed hybrid core solutions that keep user plane data within the enterprise NPN while enabling control plane data egress to the service provider. In this manner, the management and configuration complexity is largely transferred to the service provider, leaving the customer to use the Private Network in similar fashion to how it would use a Wi-Fi network.

While Private Networks have been heavily reported on in the media over the last 3 years, there is still a lack of education in the enterprise community. The benefits of Private Networks are broadly known: QoS, performance and reliability are well-understood concepts and have contributed heavily to the rising enterprise interest in deployments. Nevertheless, further education on the nuances of the market is still required in terms of:

- How the customer can enter the ecosystem, and what types of players they will be working with.
- How the project is financed – what Capex is required, what managed services will be delivered.
- Differences between operational models – can, and should, the enterprise go down the standalone, self-managed route? Is a managed service model more effective, or is a fully-fledged network-as-a-service model the right path?

- How should connectivity be addressed – if there is a need for device connectivity across public and private networks, how can this be addressed, and what is the best fit route to take to ensure that expectations are met?
- What sort of timelines and milestones can be expected by customers, and how are roles and responsibilities assumed by both the customer and the service provider?

Partner Engagement

Although it may sound cliché, engaging with the right ecosystem partners is fundamental to the deployment and operation of a successful LTE or 5G Private Network project; perhaps more so than in other services. This is due to the fact that enterprise requirements are inherently bespoke, and require both expertise and experience in deployments. Indeed, Air France's Christian Regnier, enterprise technical architect for critical wireless, stated:

> ***"Traditional network operators, as well as network vendors, don't have the in-house expertise to serve the enterprise market with industrial-grade private LTE and 5G networking. They need hand-holding by market specialists, in the form of enterprise customers and system integrators, if they are to be any more than a conduit for networking gear."***

As exemplified by Air France's experience, partners must understand that radio network design and deployment is, unless a slice of public mobile radio is used, different to how deployments are traditionally approached for countrywide mobile network provisioning. As such, selected partners in this domain must be able to combine radio expertise with knowledge and understanding of the environment in which the Private Network is deployed, whether this is a logistics or transportation hub, or a manufacturing site. In turn, these partners will be able to help the customer understand whether an LTE network is suitable for its needs, or if 5G technology is required. The path chosen is likely to be heavily dependent on the bandwidth requirements of the site, in addition to a clear understanding of how operations at the site are likely to develop in future. Should LTE be selected for the network, it is important that the core network solution is upgradeable to 5G via a software migration path: this will ensure that hardware costs are minimised, while delivering a future-proof deployment.

Connectivity

Naturally, connectivity forms a core element of the overall solution, and experiences can vary depending on the type of partner selected. Decisions made should, in the first instance, rest on whether:

- Inter-site connectivity is required where, for instance, data from more than one Private Network can be shared with another.
- The level of mobility required for devices entering and leaving the Private Network area. In many cases, these devices will require connectivity after they have left the Private Network.

As we can see from the points above, full network isolation is not only undesirable in some instances, but also prevents the extraction of the most value from a Private Network deployment. As noted earlier, most early Private LTE projects have focused on full-isolated solutions that do not take advantage of inter-site connectivity or allow mobile devices to authenticate across public and private networks. There are 2 principal reasons behind this:

- Early Private Network customers have demanded the highest security requirements for their projects, meaning that all traffic must be fully isolated from the network. Additionally, the immature state of the cellular Private Network market has meant that relatively few companies have established several sites requiring interconnectivity.
- Although mobility may well be recognised as beneficial by the customer, the enablement of public-private network access is a challenging task.

Security & Traffic Routing

The main reasons behind the deployment of a Private LTE or 5G network are the ability to ensure specific QoS and throughput for devices, as well as to ensure that business-confidential data remains confidential. In both instances, these are factors behind the shift from enterprise Wi-Fi to Private LTE or 5G.

Security in terms of network authentication is built into the 3GPP's cellular standards, and relies on hardware-grade security in the form of the UICC or eUICC (removable, traditional SIM cards or more modern eSIMs which can take any form factor). SIM card security is hardened and assured from an end-to-end standpoint and is extremely difficult to compromise. For this reason, the device-based authentication used in LTE and 5G is superior to Wi-Fi, where the breach of a user's credentials to access the network is a relatively simple task.

Meanwhile, networks must ensure that traffic produced by devices are only transported to end points that the business customer deems appropriate. In almost all cases, this will mean that traffic on the data plane (sensor data, video content, messages and so on) must only circulate inside the Private Network, and not be transported across the public Internet. Where data plane traffic does leave the Private Network, it must only do so to reach another secure, business-authenticated endpoint.

Where control plane data (the signalling traffic that monitors and manages the overall function of the network) is concerned, in many instances it is desirable to allow this traffic to leave the Private Network zone to core network infrastructure located elsewhere; usually in the cloud.

The primary reasons behind this are to enable lower costs, by not having to deploy expensive core network software and hardware on-site, while cloud-based core network architecture can be 'spun up' and configured in a much faster time than on premises configurations. Naturally, this means that the ability to separate control plane and data plane traffic is fundamental to the security and proper operation of the Private Network. Mechanisms for this are built into LTE and 5G, although they require third party expertise to monitor and manage this implementation.

Roaming & Roaming Hubs

The international nature of IoT as well as workforce sourcing, particularly in manufacturing and transportation use cases means that devices in question may originate from several different places in the world. Rather than source local SIM cards and arrange connectivity agreements with several MNOs across the world, complexity can dramatically be reduced by sourcing a global roaming solution through a competent Connectivity Service Provider (CSP). The CSP will typically issue businesses with SIM cards, which are supported by both domestic and international roaming agreements. In this manner, coverage and connectivity uptime are maximised for the customer, while contractually, only a single service provider is engaged with to provide an international connectivity solution.

While many providers have multiple bilateral agreements to facilitate roaming, these are often complex and time-consuming even for established CSPs to navigate and extend the footprint where required. Essentially, an enterprise customer using the bilateral agreements set up by a single CSP is unlikely to receive optimum coverage or performance for its devices all over the globe. More recently, roaming hubs have been established which provide a centralised touchpoint for access to roaming.

In this context, the roaming hub provider is the entity responsible for establishing and managing any number of roaming agreements, although the customer is in turn able to access all of the agreements in place with members of the hub. This model greatly increases the number of potential networks that the enterprise can access. Meanwhile, the scale of traffic flowing across the roaming hub means that the roaming hub CSP is often in a position to negotiate favourable wholesale access rates, which in turn may mean a lower connectivity cost at retail for the enterprise customer.

Local Breakouts

Where mobility is desired so that devices can authenticate with both public and private network infrastructure, factors such as performance, compliance and regulation come into play, and may mean that the customer requires a fully local deployment in terms of network access and traffic routing when roaming.

Interconnect providers have developed so-called 'breakout' models, with gateways deployed on a country or regional basis. Rather than 'tromboning' traffic to the home network provider and back to the device as is the case in a traditional roaming scenario, traffic is routed via a local or regional packet gateway, offering not only reduced latency, but also the ability to meet business or regulatory compliance requirements in terms of cross-border data flows.

Coordination of Public-Private Network Access

One of the most challenging aspects to manage for a Private LTE or 5G solution is the aspect of mobility: ensuring that devices that move in and out of Private Network coverage connect to either the public or private network in an appropriate, seamless manner. At this stage, it is important to note that, in the vast majority of cases, the public radio signal will overlap the Private Network's coverage zone. Therefore, how will a device know that it should switch its network access over to the Private Network? Under a typical scenario, this handover is achieved in a non-deterministic manner that in many cases will result in devices remaining connected to the wrong network, thus potentially disabling access to certain apps that can only be used when connected to specific networks.

Seamless handover between networks requires that the service provider has integrated the public network with the private network in a manner that enables deterministic network switching. Here, it is important to establish whether the provider is, in the first instance, technically capable of achieving this and secondly, at what cost.

Alternatively, dual SIM, dual-IMSI or eSIM can be used to ensure that appropriate network access is provided. In this case, eSIM offers the modern and most flexible solution, as network access credentials can be delivered over the air. Authentication to the networks can then be achieved either in manual fashion, which is naturally not possible for machines or assets that require seamless connectivity, or via embedded intelligence in the form of an applet residing on the SIM card.

Strategic Recommendations

Enterprise Private LTE and 5G networks offer customers a considerable step-up in terms of quality, reliability and flexibility over other technology solutions deployed in the past. While the cost of entry can be high, where full network isolation and a fully on-premises deployment are required, customers that are confident in the security of a cloud-based, network-as-a-service model will find that Capex is much less of an issue. As outlined in this report, choosing how to deploy the network or even choosing whether to deploy an LTE or 5G solution at all, is dependent on the overall business's needs and future requirements. Therefore, in this section Kaleido will highlight key recommendations for enterprise customers that are considering a Private LTE or 5G deployment.

Evaluate if Private LTE or 5G is Appropriate for the Business

Although it is often stated that LTE and 5G base station coverage is superior to Wi-Fi, requiring fewer overall hardware access points (APs), cellular network hardware comes at an additional cost over Wi-Fi APs. In addition to this, LTE and 5G come with complexities that normally present challenges for enterprises in terms of network management and configuration. These complexities undoubtedly provide enhanced control and reliability, but will require the expertise of a third-party managed services provider in most instances. By and large, enterprises are very familiar with Wi-Fi, and as such, have already priced in the cost of network management through their existing in-house IT expertise.

It must be understood that Private LTE and 5G are not direct competitors to Wi-Fi. These technologies are appropriate for specific use cases, where, in general:

- Wi-Fi is a relatively low-cost solution suitable for general-purpose commercial operations. A lower overall reliability in terms of connection quality means that operations relying on real-time data flows or high availability should avoid Wi-Fi if possible.
- LTE and 5G offer high-reliability, high availability services at a higher cost. Typically Private LTE or 5G is used when the business requires support for critical operations that must not suffer from connection dropouts or dropped packets.

Evaluate the Connectivity Model for Private LTE or 5G

Private LTE and 5G networks can support a variety of connectivity models including those that simply require connectivity inside the Private Network coverage zone, inter-site connectivity as well as mobile device or asset connectivity across public and private networks. The level of mobility required dramatically changes how the enterprise must go about planning and selecting partners for the deployment:

- Fully isolated solutions are the simplest to deploy from an interconnection standpoint. No roaming or outbound data flow is required, and only SIM cards registered to the Private Network will be allowed to operate inside the network. A large number of players exist on the market today with experience and expertise in deploying these types of networks.
- Deployments requiring inter-site connectivity will most likely require partnering with a CSP capable of supporting international transport across secure links with guaranteed service levels. If required, this partner may in future be in a position to support connectivity enablement across public and private networks on an international scale. Typically, these types of players are IPX providers, although a smaller number of Private Networks solutions providers have the capability to support this type of deployment directly.
- Customers which require seamless connectivity across public and private networks must consider partnering with a CSP with an international connectivity footprint as well as the technical expertise to support one of the authentication mechanisms discussed earlier in this report in a robust and cost-effective manner. Some IPX players are capable of addressing this side of the market, either directly, or via partnerships with specialist IoT connectivity service providers.

Evaluate if LTE or 5G is More Suited to the Private Network

While much of the discussion around Private Networks today centres around 5G technology, LTE offers a viable solution for deployments in many instances. 5G does offer advantages, notably in terms of the number of connections supported per cell, as well as higher throughput rates, which is one of the reasons why demand for 5G is growing in the manufacturing and industrial sector. Nevertheless, support for 5G in the overall ecosystem is still growing, with the choice of modems, devices and radio equipment not yet as developed as it is for LTE. Although 5G is often talked about in terms of very low latency, careful design of a Private LTE network can, in some cases, achieve very similar latency levels without the extra expense involved with 5G technology.

It is important to understand that, in the first instance, 5G is backwards compatible with LTE and secondly, core network solutions that are '5G ready' merely require a software upgrade to support 5G operations as needed at a later date. Therefore, entry into the market using LTE is a viable option, given that transitioning to 5G will not require swapping out the entire device base inside the network due to backwards compatibility. Additionally, the software upgrade path helps lower future costs, which is in contrast to other types of private network communications technologies, which normally require a complete hardware upgrade.

About the Authors

BICS is a leading international communications enabler, one of the key global voice carriers and the leading provider of mobile data services worldwide. Its solutions are essential for supporting the modern lifestyle of today's device-hungry consumer – from global mobile connectivity, seamless roaming experiences, fraud prevention and authentication, to global messaging, and the Internet of Things.

BICS's SIM for Things, the global connectivity platform for IoT offers customer one SIM, one platform, one global partner, delivering:

- Mobile connectivity for any IoT deployment in over 200 countries with multi-network mobile coverage in six continent
- Reliable, high-quality worldwide infrastructure, patented roaming technology and global presence
- All platform functionalities are available through a growing library of more than 210 flexible and easy-to-use APIs
- Greater visibility of device connectivity, usage patterns, and quality of service with BICS' SMART for SIM for Things – track a wide range of parameters to control and optimize any large-scale connected business

Kaleido Intelligence

Kaleido Intelligence is a specialist consulting and market research firm with a proven track record of delivering telecom research at the highest level. Kaleido provides insightful business analysis, market projections, recommendations and growth strategies for global mobile operators, telecom vendors and IoT service providers.

Kaleido is the only research company addressing mobile roaming in its entirety, covering industry leading market intelligence and publications on Wholesale Roaming, IoT Roaming, 5G Roaming, IPX and Analytics & Fraud in Roaming. Research is led by expert analysts, each with significant experience delivering insights that matter.

Publication Date: January 2022

For more information on this market study or if you have further requirements, please contact:
+44 (0)20 3983 9843| info@kaleidointelligence.com

Kaleido aims to provide accurate information. The information provided here is designed to enable helpful data and insights on the subjects discussed. References to companies are provided for informational purposes only and Kaleido does not endorse any operator, vendor or service included in this research and market study. While information and content of this publication is believed to be accurate at the date of publication, neither Kaleido Intelligence nor any person engaged or employed by Kaleido Intelligence accepts any liability for any errors, omissions or any loss or damage caused or alleged to be caused directly or indirectly by what is contained in or left out of this publication. This report consists of the opinions of Kaleido and should not be construed as statements of fact. It contains forward-looking statements and market forecasts that have been developed based on current information and assumptions. These are subject to market factors such as, but not limited to, unforeseen social, political, technological and economic factors beyond the control of Kaleido Intelligence.