Security Concerns in Private Wireless Deployments

Pathfinder

January 2022

Commissioned by

Betacom

451 Research

S&P Global
Market Intelligence

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About the Author

Eric Hanselman

Principal Research Analyst

Eric Hanselman is the Principal Research Analyst at 451 Research, a part of S&P Global Market Intelligence. He has an extensive, hands-on understanding of a broad range of IT subject areas, having direct experience in the areas of security, networks, application and infrastructure transformation and semiconductors. He coordinates industry analysis across the broad portfolio of 451 Research disciplines, contributes to the Information Security and Cloud Native Channels, and is a member of the Center of Excellence for Quantum Technologies.

The convergence of forces across the technology landscape is creating tectonic shifts in the industry, including 5G, SDN/NFV, edge computing and DevSecOps. Eric helps 451 Research's clients navigate these turbulent waters and determine their impacts and how they can best capitalize on them. For more than 20 years, Eric has worked with segment leaders in a spectrum of technologies, most recently as CTO of Leostream Corporation, a virtualization management provider. Prior to that, Eric guided security offerings for IBM and Internet Security Systems. At Wellfleet/Bay Networks and NEC, he was involved in the introduction of many new technologies ranging from high-performance image analysis to rollouts for IPv6.

Eric holds a patent in image compression systems. He is also a member of the Institute of Electrical and Electronics Engineers (IEEE), a Certified Information Systems Security Professional (CISSP) and a VMware Certified Professional (VCP), and he is a frequent speaker at leading industry conferences. Eric majored in Chemistry at Reed College.

Executive Summary

Many organizations are considering how they can take advantage of private wireless 4G and 5G networks. Their focus is often on the cutting-edge technologies, which can offer significant business benefits, but it's important not to lose sight of the operational aspects of these opportunities.

Security is often cited as a primary driver for private wireless, but enterprises are also reporting that they're struggling to maintain security in their existing infrastructure – with technologies they know well. Private wireless deployments are going to need enhanced security support to enable enterprises to realize their benefits without overwhelming their in-house security teams.

Key Findings

- Private wireless offers significant benefits for enterprises that are looking for secure, scalable connectivity.
- Operational aspects for private wireless deployments should be a prime consideration.
- Most enterprises face key skills and staffing gaps in security.
- Automation and AI augmentation can help speed security responses and scale security management.
- The threat landscape for wireless networks is evolving rapidly, and considerable investment is required to stay ahead of attackers.
- Managed private deployments can deliver benefits without overburdening security teams.

Introduction

Advances in wireless technology are making it practical for enterprises to consider tapping the benefits of private wireless networks for their businesses. An expanding ecosystem of vendors, enterprise-ready deployment options and simplified operational models are all helping to make this option a reality. There are many benefits to private wireless cellular deployments, including improved security compared with typical Wi-Fi installations, greater control for deployed environments and the ability to operate at much greater scale.

Enterprises can face challenges as they strive to achieve those benefits, though, if they face the skills shortages that have become common in security management. There are paths forward that can help them overcome these challenges and build successful deployments, if they choose carefully and build on a foundation of solid partnerships.

Benefits of Private Wireless

Most organizations are familiar with the operational complexity that is typical of Wi-Fi deployments. While great strides have been made in applying improved management and operational capabilities to Wi-Fi, there are still significant advantages that wireless cellular technology holds over it.

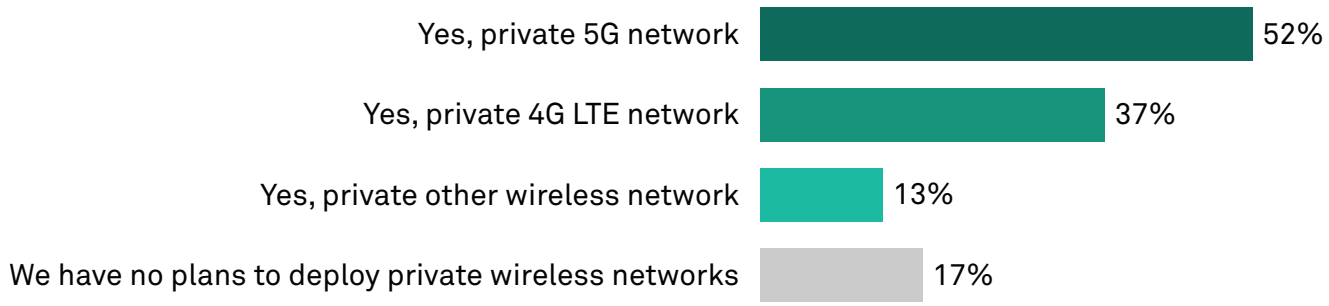
Security is an area where wireless has a clear lead, in that identity and access management was designed in from the start, rather than overlaid after the fact. Wireless can also provide access to dedicated radio spectrum that removes much of the competition that exists in Wi-Fi, and 5G wireless adds the benefit of spectrum slicing that can allocate private deployments their own bands in which to operate and increase access control.

The control capabilities that private wireless offers can simplify operations by leveraging the device identity that's fundamental to its operation to manage policies for connectivity, access and performance. Native capabilities ensure that enterprises can control who and what is on their network and manage their access more directly.

Private wireless' ability to operate at greater scale stems from the nature of its design. It's based on technology that is built to support large universes of devices and their users. An expectation of greater scale means that operational management is supported with greater levels of automation, which can reduce the organizational burden in terms of staffing levels.

It's not surprising, then, that enterprises are looking to private wireless networks to address their needs for a connectivity solution that gives them the security, control and scale they require. In a recent 451 Research Voice of the Enterprise (VotE): Internet of Things study, 83% of survey respondents said they were planning to use private wireless technology in some form.

Figure 1: Planned Usage of Private Wireless Technologies



Q: Does your organization plan to use any of the following private wireless network technologies as part of its IoT infrastructure deployment? Please select all that apply.

Base: All respondents (n=567)

Source: 451 Research's Voice of the Enterprise: Internet of Things, The OT Perspective, Technology & Vendor Decisions 2021

Private Wireless Use Cases

Private wireless is attractive for a wide range of applications, and some of these are particularly useful in illustrating the major benefits that it can deliver to specific industries. A requirement for secure, scalable connectivity is the common thread that runs through all the use cases we examine here.

Transportation

There are extensive needs for robust connectivity in the transportation industry, but probably none more comprehensive than in aviation. There is an intersection of the needs of safety, security and high-performance connectivity that private wireless is particularly well suited to address in this sector. Airports can be vast and sprawling physical environments with a mix of passengers and staff that require very different levels of service and access.

Location and access information is tremendously valuable, and airport operators have valid concerns about exposing it on public networks. The modern airport encompasses retail and hospitality services along with airline operations, and their needs around PoS terminal connectivity and traffic data are key. Baggage handling needs are also well established, and as airlines grow, so do their requirements for aircraft data transfer for flight data management (FDM), entertainment systems and flight operations quality assurance (FOQA), as well as demands for high capacity and high security at the gate.

Warehousing and Logistics

One of the most significant lessons of the global pandemic is around the importance of robust supply chains. Warehouses and logistics operations are on the front lines in terms of ensuring that materials get to where they're needed, and thus have extensive requirements for connectivity that has both scale and capacity.

These workers also generate large amounts of valuable data about the goods they're handling – information they would prefer to control directly. The ability of private wireless networks to scale across warehouses and storage yards, while still securing network traffic, allows warehouse operators to meet those needs and maintain this control. Data from scanners, materials handling systems, security cameras and vehicles can all be integrated with the policy controls that private wireless is uniquely suited to deliver.

Manufacturing

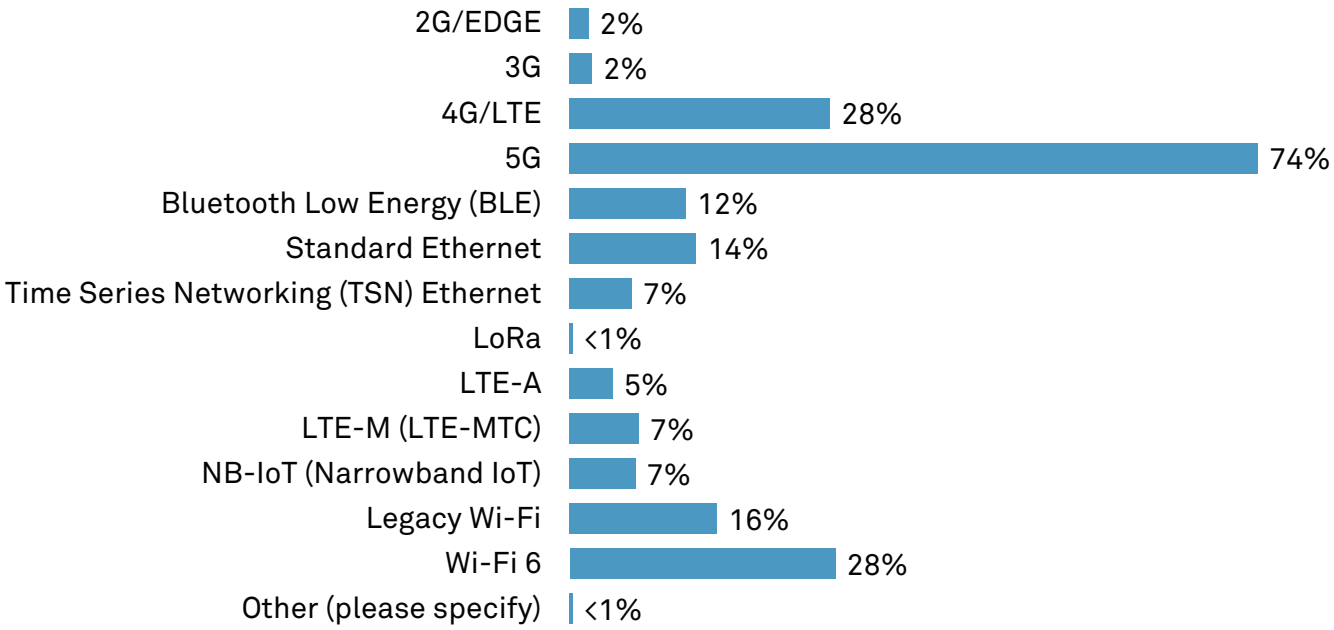
While there are many industries being transformed by digitization, the shift in manufacturing known as Industry 4.0 is a high-profile example of the types of improvements that are possible in an industry that hasn't always been seen as a leader in IT adoption. What is less well known is the extent to which Industry 4.0 depends on reliable connectivity to realize its goals.

The factory floor has become a source of new volumes of data, but that data has to be reliably fed back into systems for analysis in order to be useful. At the same time, agile manufacturing techniques often require that reconfiguration be easy and fast. The fixed, wired networks used in the first waves of industrial digitization are too constrained and costly to keep up with modern requirements. It's also an environment where the data and control traffic that runs over the network has to be well secured to prevent eavesdropping and defend against attacks.

Technology Trends

When considering the technology to support private wireless deployments, there's always a temptation to focus on the latest and greatest advances, and this is an area that merits special consideration because of the complexities involved. Many enterprises are expecting to rely on 5G technologies, as the results of a recent 451 VotE IoT study show. Survey respondents indicate a dramatic shift to 5G in the next two years. This illustrates the massive enthusiasm for 5G, which may be driven in part by consumer-level rollout activity.

Figure 2: Network Connectivity Technologies Usage in Two Years



Q. Looking ahead, which of the following network connectivity technologies do you expect your organization will primarily use for its IoT connections in two years? Please select all that apply.

Base: All respondents (n=537)

Source: 451 Research's Voice of the Enterprise: Internet of Things, The OT Perspective, Technology & Vendor Decisions 2021

The advantage of a private wireless deployment is that organizations can consider the factors most important to their specific application in selecting the technology they deploy. The 5G ecosystem is maturing rapidly, but still has limitations in terms of the form factors and costs of network equipment, as well as the devices that are available to connect to it. Depending on the application, it can make sense to deploy LTE initially to manage cost and schedule targets, and then upgrade to 5G later as required. Deploying upgradable equipment can maximize the flexibility of the network design.

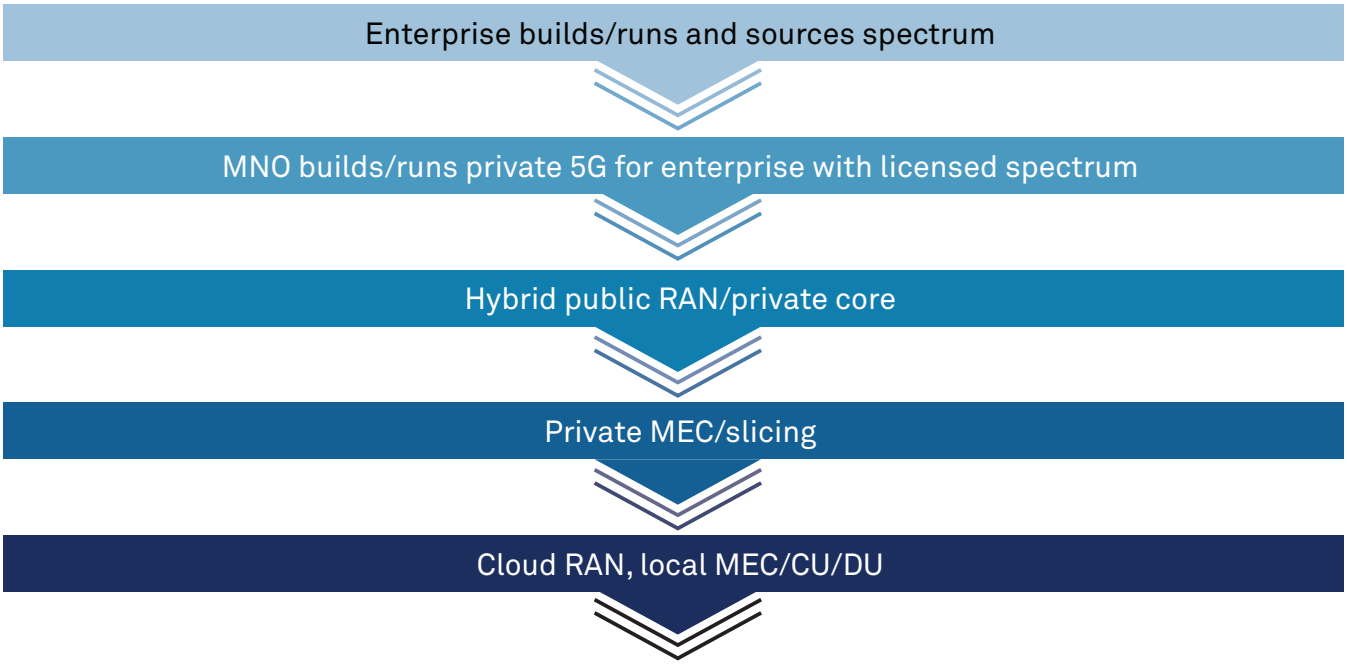
Enterprise Expectations for Private Wireless

There are also many choices around the way in which private wireless network services are delivered. Deployment models range from those that are fully owned to those that are fully virtualized. There are vendor offerings that can allow an enterprise to completely buy, build and manage the network, but this option requires staffing and skill levels that would be prohibitive for most organizations. There is also the question of how radio spectrum for running the network will be acquired, which can be complex and expensive for organizations without fluency in these areas.

For most enterprises, some level of managed offering will make sense. Fully managed offerings from mobile network operators (MNOs) provide private service over shared infrastructure. This is an arrangement where all of the operational systems would be controlled and managed by the operator. It has the benefit of relieving the enterprise of any network equipment management, but doesn't address the data security concerns that drive many organizations to private wireless in the first place.

There are variations in delivery models where the radio access network (RAN) is shared in a hybrid approach that can allow an enterprise to have the network core or edge under its control, but these also wouldn't meet a requirement to have a fully private network path. These approaches also typically depend on existing tower installations, which may not offer the necessary levels of coverage.

Figure 3: Private 5G Deployment Options



Source: 451 Research, part of S&P Global Market Intelligence

Choosing a managed deployment where the enterprise owns and controls the physical infrastructure but the operations are managed remotely can meet the requirements that many have for operational integration while also addressing any concerns about data locality. In this type of arrangement, the managed service provider attends to the design, spectrum and deployment of the network, allowing it to be tailored to the needs of the application and the site.

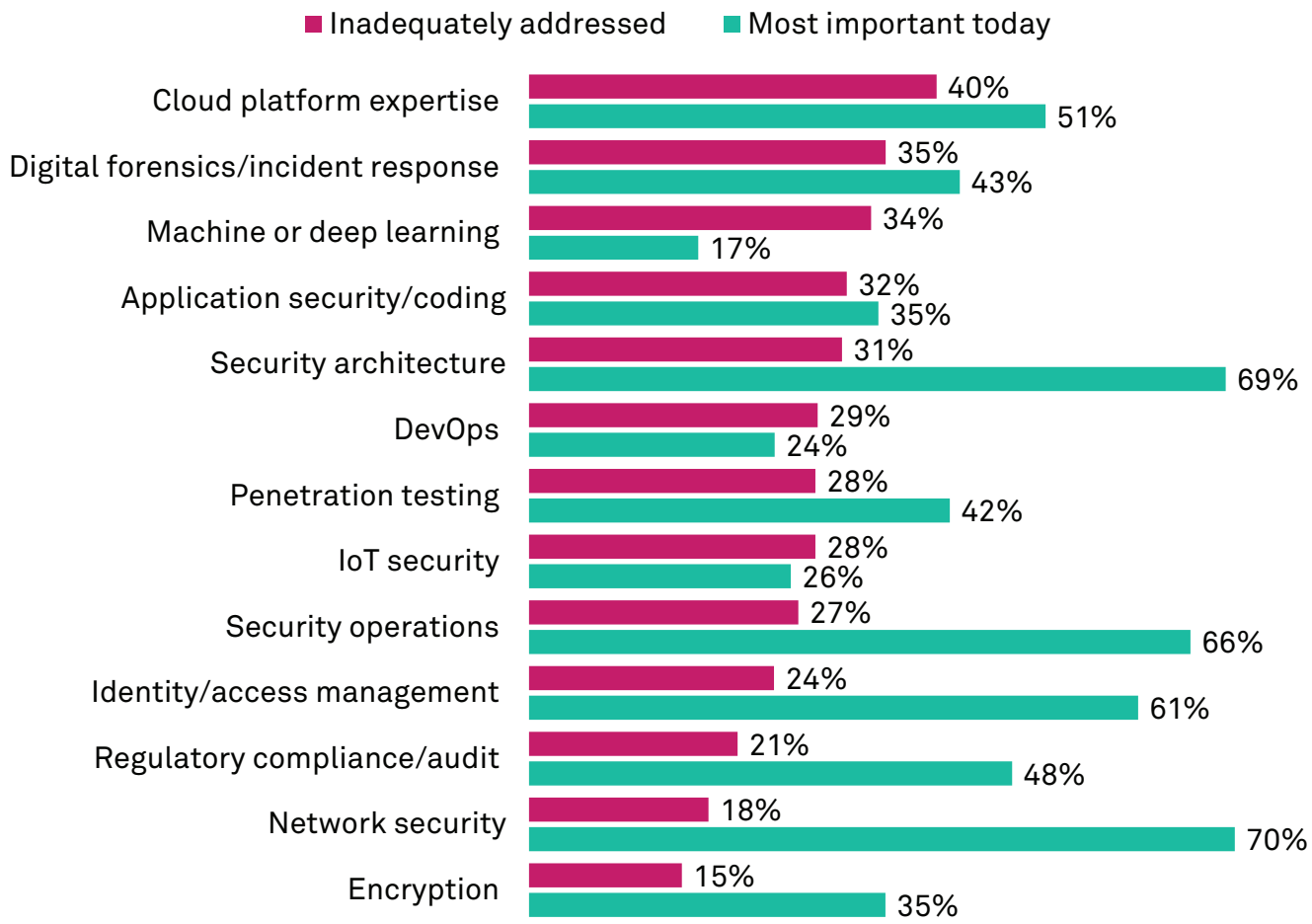
This is an option that allows network elements to be deployed more flexibly. It allows on-premises datacenter capacity to be used and also supports public or private cloud deployments. The decision on where to host the equipment is typically driven by the level of flexibility needed and any security constraints. Cloud deployments offer the ability to easily expand capacity and manage cost. On-premises deployments have the benefit of fixed cost, but with some loss of agility. This is a deployment option where the enterprise not only gets tailored wireless connectivity, but also full ownership of the data that the network generates.

In any deployment configuration, organizations will need to consider the security operations aspects of their environment. Wireless networks bring a set of security concerns that may not be familiar to most enterprises. It's an area where any management provider will have to be skilled in not only the operation of the network, but also the integration with the enterprise and its environment.

Overcoming Enterprise Challenges

While the advantages are significant, the average enterprise faces a number of challenges in integrating the capabilities of a private wireless network into their operations. The most significant of these is security. The typical enterprise faces chronic gaps in security staffing and skills. Adding the new technologies and attack surfaces involved in a private wireless network could mean even more strain. In a recent 451 VotE Information Security study, respondents listed a range of skills gaps that could present challenges when integrating the new infrastructure to support a private wireless network.

Figure 4: Most Important Skills for Security Professionals vs. Most Lacking



Q. Which of the following skill sets are most important for security professionals to have today? Please select all that apply. (n=435) Q. And which skill sets are inadequately addressed at your organization today? Please select all that apply. (n=415)

Base: All respondents

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2021

The greatest concern for most organizations will be the ability to scale their security operations to the level needed to effectively secure this new element of their infrastructure. It also requires levels of automation in security operations that are beyond what is in place at most enterprises. A majority (53%) of the VotE study respondents said their current security staffing levels are already inadequate for their current environments, leaving little capacity to take on new tasks.

There are various capabilities that must be put in place to overcome these challenges. The first of these is building new sources of threat intelligence, with the ability to apply them to anticipate new attacks. Wireless threats extend into tactics, techniques and procedures that are beyond the scope of most enterprises' security mandates, so some learning is required here.

Meanwhile, automation offers a means to deal with the scale and speed of action that wireless networks require to both identify issues and remediate them. This is an area where it's simply not possible to address threats manually. Machine learning and artificial intelligence (ML/AI) can be force multipliers for security teams when these technologies are properly applied. They require models built with the specialized knowledge of wireless operations, and they must be integrated with the automation driving security operations.

An additional factor that can aid enterprises in managing private wireless security is the establishment of operational segmentation between core business functions and the operational network. These two spheres are distinct enough in nature so there is little benefit in blending them, as long as there is good functional integration. The connectivity pieces of the wireless network and the telemetry it provides can be fed directly into the IT systems of the enterprise without adding significant work to admin teams. Data generated by the network can be integrated as new data sources into existing analytics and security platforms. This type of approach delivers value without requiring reskilling existing staff.

A Better Path Forward

The means to overcome existing enterprise challenges can be built within an enterprise, but that may not be the most efficient path when time and cost are considered. Working with a partner that already has the skills and capabilities to manage a private wireless network has the potential to not only accelerate deployment, but also deliver better time to value if the partner can manage integration. The partner must be able to deliver the network in the form and design that best suits the organization's requirements, and operate it with a model that fits its specific needs and operational style.

There are a number of options in the types of partner relationships in the market today, and finding the right fit in a partner is a critical factor in the success in any deployment. As discussed earlier, MNO/MVNO relationships, where the delivery network is owned and managed by the partner, won't meet the requirements for most organizations looking at private wireless. Meanwhile, the shared infrastructure model simply won't meet their security needs.

Telecom equipment vendors have early-stage offerings on the market, but they typically expect the organization to manage a significant part of the operational and security aspects of the network. There are some network operators starting to offer services, but this is an adjunct to their core business, and organizations will need to carefully consider the levels of support and commitment, as well as technical flexibility, they will be able to offer. Deployments that don't fit their existing blueprints may be challenging for these operators.

To realize the full benefits of private wireless, organizations must be able to achieve their security goals alongside the ability to put operational data to work, while limiting operational complexity. It's a delicate balance, but one whose rewards are worth the planning efforts required to make it happen.

Conclusion

Enterprises can effectively realize the many benefits of private wireless cellular networks when they take a path that enables them to gain the inherent advantages while minimizing the complexities of this powerful resource. The ability to maintain control of valuable data while ensuring the security of the environment can give them the double benefits of upside value and operational simplicity. Effectively managing access security with targeted security policies can move enterprises far beyond the limitations of Wi-Fi.

Being able to fully control the network from end to end and deploy infrastructure in ways that meet their specific security, regulatory and operational requirements will enable enterprises to tap the full potential of their data assets, with levels of security that are hard to achieve in any other way. Working with a capable partner that can both deliver a wireless network and ensure its security in a manner that doesn't overburden in-house security teams will allow enterprises to enjoy the scale, security and performance that private wireless offers.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence