IMAGINE WIRELESS

Use Case Spotlight:

Airport Perimeter Connectivity

The Challenge

While airports are as distinct as fingerprints, they all share a small set of essential defining attributes. These include one or more of the following: a runway, a control tower, a terminal building, aircraft maintenance and storage facilities, and parking facilities. These are the "objects within the square" of the property, so to speak. What is less often the focus of the conversation is the square itself… the airport perimeter.

The airport perimeter is more than simply the property boundary line. It is a security perimeter that controls access to sensitive areas that require constant, effective security oversight. There are generally also multiple sensitive areas demarcated within the airport grounds. The airport operator is obligated to monitor and control it all, for the safety of passengers, workers, national airspace, and international airspace. Prominent security breaches over the decades illustrate the consequences of inadequate perimeter security and underscore the importance of establishing and maintaining an effective posture.

Fencing, even multiple layers of fencing, is not enough. Robust physical security is enhanced by the addition of effective digital security, which takes the form of cameras, sensors, and solutions – software applications and physical devices – that take action in the event of a potential risk or confirmed breach. The key to digital security is providing connectivity to these applications and devices across and within the airport perimeter.

Many airports have not yet evolved beyond stand-alone physical security to incorporate connected digital solutions into their security postures. Airports that have instrumented their fencing with such solutions tend to default to wired solutions – generally fiber-optic cabling or Ethernet cabling. Yet physical cabling of any type is expensive to deploy, repair, operate, and reconfigure. This cost barrier can lead to incomplete or inadequate connectivity and the security risks that come with it.

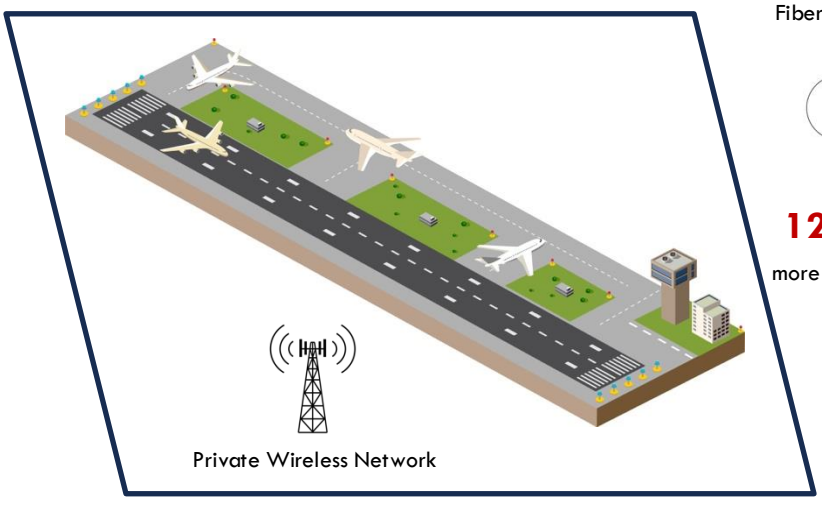
Connectivity to secure the airport perimeter…

… PWN offers the only reasonable choice.

Ethernet Cabling

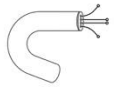
5x – 7x

more expensive than PWN



Private Wireless Network

Fiber-Optic Cabling



12x – 18x

more expensive than PWN

Cost reflects total cost of ownership, equal to initial CapEx + OpEx over 5 years. Figures based on Imagine Wireless researchand client experience.

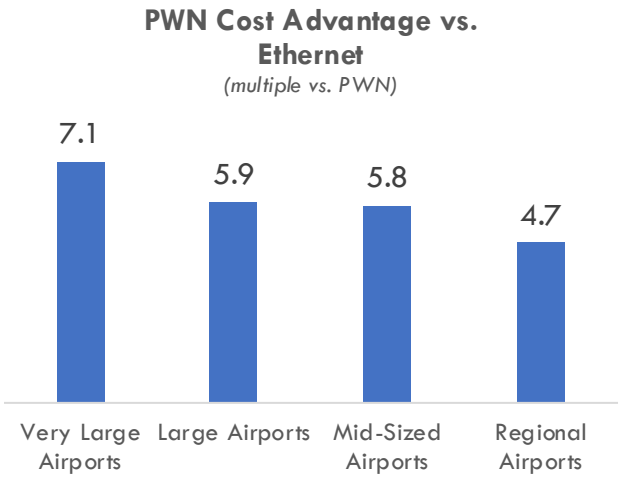
The Solution

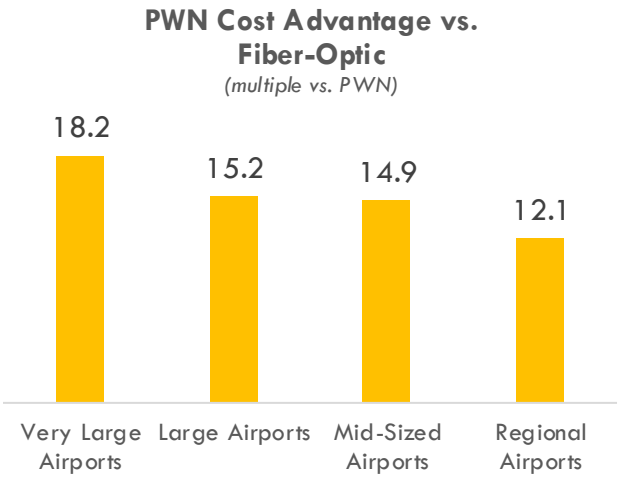
While physical cabling can provide the connectivity that airports require to implement, operate, and evolve a secure physical perimeter, cabling cannot do so in a cost-effective manner. Wireless technologies, specifically wireless wide-area networks (WWAN), offer the most agile and cost-effective solution.

Privately-owned WWAN, or simply Private Wireless Networks (PWN), offer an additional degree of agility and cost-effectiveness for airports, since the airport owns and operates the network equipment instead of paying a mobile network operator (MNO) to do so. The cost savings of PWN are evident immediately and accrue substantially over time.

Business Impact

Analysis of the PWN cost advantage over fiber-optic and Ethernet cabling illustrates the extent of the savings opportunity for airports of different sizes:





Expressed as total cost of ownership (initial capital expenditure + operating expense over 5 years), Ethernet cabling is 5x– 7x more expensive than PWN, while Fiber-Optic cabling is 12x – 18x more expensive.*

PWN for perimeter connectivity drives savings in the form of foregone capital expenditures and operating expenses, liberating cash flow that the airport operator can redeploy for other purposes.

Learn More

There is a right way to digitize the airport perimeter – through PWN. How can PWN help your airport achieve its perimeter connectivity and security objectives? Let's talk and explore the possibilities.

Contact us to start the conversation. Imagine Wireless.

** Cost reflects total cost of ownership, equal to initial CapEx + OpEx over 5 years. Figures based on Imagine Wireless research and client experience.*