



## INDUSTRY INSIGHT: **DATA PRIVACY MATTERS**

Comparing Cellular and Wi-Fi connectivity  
for a safer connected experience.

dense air

# Introduction: Cellular vs Wi-Fi



In today's digital age, staying connected is essential for individuals and businesses alike. However, connectivity comes with inherent risks to privacy and data security. For businesses, these risks can manifest as customer privacy breaches, compromised productivity, operational disruptions, or even massive financial losses. Additionally, connectivity in public spaces introduces further vulnerabilities to individuals, enterprises, and the public sector.

As we observe Data Privacy Week, January 27–31, 2025, it is critical to explore the security implications of the two most used connectivity options: Wi-Fi and cellular networks. This comparison becomes even more significant when evaluating security for staff using BYOD (Bring Your Own Device) policies, carriers mandating network security, and building management running critical operational use cases.

**1/3** OF GLOBAL CELL USERS  
HAVE HAD A **DATA BREACH**

EMARKETER, 2022: Thales Consumer Digital Trust Index

# Index

---

**01**

## **Introduction:** Cellular vs Wi-Fi

### **Public Wi-Fi:** A Convenient Risk

Key Risks of Public Wi-Fi

Implications for Key Use Cases

**02**

### **Cellular:** A Safer Experience

Addressing Risks in Specific Use Cases

Potential Risks of Cellular Networks

**03**

### **Final Word:** Prioritizing Security in Connectivity Solutions

**cellShare®:** Secure Cellular Connectivity

# 1. Public Wi-Fi: A Convenient Risk

Public Wi-Fi networks are ubiquitous in cafes, airports, libraries, shopping malls, and more. While they offer a convenient way to connect to the internet without consuming data plans, this convenience comes at a significant cost in terms of security.

Public Wi-Fi networks are often unsecured and easily accessible to anyone within range, including bad actors. They frequently lack proper encryption protocols, making data transmitted over these networks highly susceptible to interception. This lack of security creates a perfect storm for cybercriminals to exploit personal data, private information, financial details, and more. Additionally, public Wi-Fi networks often allow unrestricted access without robust authentication, increasing the risk of unauthorized access to connected devices.

## 1.1 KEY RISKS OF PUBLIC Wi-Fi

### **Man-in-the-Middle Attacks:**

Hackers can intercept data transmitted between a user and the Wi-Fi router, capturing sensitive information such as login credentials, financial data, and personal messages.

### **Rogue Hotspots:**

Cybercriminals can set up fake Wi-Fi networks that mimic legitimate ones. When users connect, their data can be stolen, or their devices infected with malware.

### **Session Hijacking:**

Attackers can take over user sessions on websites or applications, gaining unauthorized access to accounts.

### **Data Theft:**

Lack of encryption exposes users to data theft, allowing hackers to access unencrypted information transmitted over the network.

### **Device Vulnerabilities:**

Unpatched software or open ports on connected devices can be exploited to install malware or gain unauthorized access.





## 1.2 IMPLICATIONS FOR KEY USE CASES

### **For Staff Using BYOD (Bring Your Own Device):**

Employees connecting personal devices to public Wi-Fi pose a substantial risk to corporate networks. Sensitive business data accessed over unsecured Wi-Fi can be intercepted, leading to data breaches and compliance violations.

### **For Building Management:**

Public Wi-Fi used for IoT devices, such as smart lighting, HVAC systems, or security cameras, can create an entry point for cyberattacks, jeopardizing building operations and tenant safety.



**3,200+**

**DATA COMPROMISES,  
AFFECTING OVER**

**353M Users**

STATISTA, 2023

## Safer with cellular



## 2. Cellular: A Safer Experience

---

Cellular networks, such as 4G/LTE and 5G, provide a more secure connectivity option compared to public Wi-Fi. These networks are inherently designed with robust security measures, including encryption and authentication protocols, making it significantly harder for cybercriminals to intercept or exploit data.

### **Encryption:**

Data transmitted over cellular networks is encrypted, protecting it from interception.

### **Authentication:**

Cellular networks require users to authenticate with a SIM card, adding an additional layer of security.

### **Network Isolation:**

Unlike public Wi-Fi, cellular networks are not accessible to everyone within range, reducing unauthorized access.

### **Carrier Oversight:**

Cellular providers actively monitor and manage network security, implementing protocols to safeguard users.



## 2.1 ADDRESSING RISKS IN SPECIFIC USE CASES

### **For Staff Using BYOD:**

Cellular networks offer a secure alternative for employees accessing corporate resources remotely. Enabling staff to use personal devices over cellular connections ensures that sensitive company data is encrypted and safeguarded from interception.

### **For Carriers:**

Telecommunications providers enforce stringent security standards across cellular networks, ensuring compliance with regulations and protecting enterprise and consumer data.

### **For Building Management:**

Cellular networks provide a reliable and secure foundation for smart building operations, reducing vulnerabilities in IoT systems and ensuring operational continuity.



## 2.2 Potential Risks of Cellular Networks

While cellular networks are generally safer than public Wi-Fi, they are not without risks:

### **Phishing Attacks:**

Mobile users are increasingly targeted by phishing scams through email, text messages, or malicious apps. Educating employees and implementing robust mobile device management (MDM) policies can mitigate these threats.

### **Malware and Ransomware:**

Apps from unverified sources or malicious websites can contain malware. Encouraging regular software updates and restricting app installations can help mitigate these risks.

### **Outdated Software:**

Devices running outdated operating systems or apps are vulnerable to known exploits. Enterprises should enforce automatic updates and collaborate with carriers to push critical patches.

### **SIM Swapping:**

Hackers can trick carriers into transferring phone numbers to their devices, bypassing two-factor authentication. Implementing stricter identity verification processes can reduce this risk.





### 3. Final Word: Prioritizing Security in Connectivity Solutions

---

As connectivity becomes the backbone of automation, intelligent operations, and critical communications, ensuring robust security is no longer optional. For businesses, the stakes are higher than ever:

**For Staff using BYOD:**

Secure connectivity is essential to protect sensitive corporate data and maintain compliance with privacy regulations.

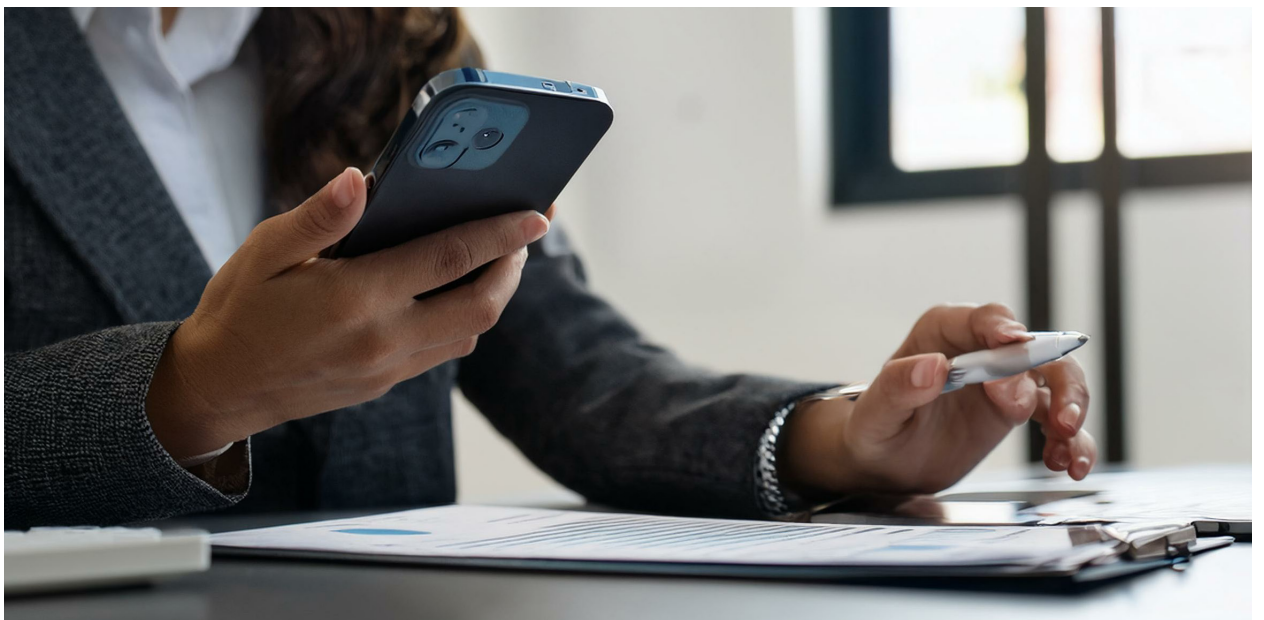
**For Carriers:**

Enforcing strong security measures across networks is critical to maintaining trust and enabling seamless enterprise operations.

**For Building Management:**

Cellular networks provide the reliability and security needed to safeguard IoT devices and maintain operational efficiency.

While public Wi-Fi offers convenience, it introduces significant risks that can compromise personal and business data. Cellular networks, with their robust security measures, present a safer alternative for both individuals and organizations. By understanding these risks and adopting best practices, businesses can protect their operations, secure sensitive data, and ensure a safer connected future.



# cellShare<sup>®</sup>

by dense air





# cellShare®

---

cellShare® by Dense Air is a unique solution that offers turnkey services to identify connectivity gaps, install hardware, implement software, and offer full-service management of cellular connectivity improvements.

Dense Air fully manages the equipment, deployment, security, maintenance, and traffic to simplify improving cellular connectivity in building. Primary details of the cellShare® solution include:

**Enabling all carriers at the same time, in the same location.**

**Cost efficient, minimal footprint and easily integrated into the existing buildings.**

**Allows for rapid installation (wks) compared to traditional solutions (mo/yrs.).**

**Ensures security, continuity, and reliability of your cellular connection.**

**Fully managed as a turnkey service**

Dense Air solves the issues of poor connections, dropped calls, and poor cellular experiences with its cellShare® solution. Installing neutral host (or multi-carrier) small cell clusters, which enhance the experience and can be installed space by space or floor by floor for multi-floor buildings allows for a customized solution that targets trouble areas and quickly improves end user experiences.

To identify where coverage and capacity gaps exist, cellShare® uses big data analytics with a proprietary software tool called denseWare® that gathers insights across multiple operators and end user activity.

Dense Air designs customized solutions and rapidly deploys small cells only where needed, utilizing existing infrastructure to limit the cost expenditure. Once cellShare® is deployed, consistent, reliable 24/7/365 performance monitoring is enabled, and maintenance and upgrade support are provided as needed.

Through denseWare®, Dense Air provides the software and APIs needed to fully integrate with existing systems, provide user and network insights, and present dashboard visibility for managers or IT teams.

cellShare® works with the existing macro network and simultaneously provides better speed and quality of experience to end users. This allows businesses to easily adapt and economically support digital transformation and transition from 4G LTE to 5G by providing indoor and near indoor small cell services to cost effectively infill coverage holes and capacity weak spots in wireless networks.





## **Key benefits offered via the cellShare® solution include:**

**Increased throughput of signal for optimal experiences**

**Reliable turnkey and white-glove service**

**Scalable and secure connectivity**

**Budget friendly solution (lower TCO, flexible opex or capex funding)**

**Less complex and faster installations**

**Integrates with top carriers simultaneously**

**Public and private wireless friendly**

**Provides location-based analytics**


As businesses digitally transform and automate, cellular remains a critical foundation for innovation. While cellular is enhancing customer experiences, it is also being used to augment, improve, or provide redundancy in enterprise or business networks.

Cellular connectivity can be used to extend or supplement businesses' primary networks, augment an existing DAS network, and be used for outdoor backhaul to enable key guest or customer services.

Utilizing the cellShare® solution opens the door for added use cases such as industry 4.0 enablement, off-loading and autonomous driving connectivity and is equipped to support a variety of use cases in both public and private wireless.

As the industry matures and slowly migrates from 4G LTE to 5G, multi-carrier, small cell solutions are a practical, flexible, cost-effective solution for key-stakeholders to enhance their connectivity.

cellShare® by Dense Air provides reliable, uninterrupted cellular connectivity for a fraction of the cost while improving overall guest and employee satisfaction, loyalty, and tenant retention. Ultimately, it maximizes your return on investment.



**A fully managed cellular solution, providing reliable in-building connectivity to conduct business and offer the guest, staff and visitor experience they expect.**



cellShare<sup>®</sup>  
by dense air

Easing the growing demand  
for cellular service through  
as-a-service small cell solutions.

For more information on  
cellShare<sup>®</sup> please contact Dense Air at:

[www.denseair.net](http://www.denseair.net)  
[info@denseair.net](mailto:info@denseair.net)