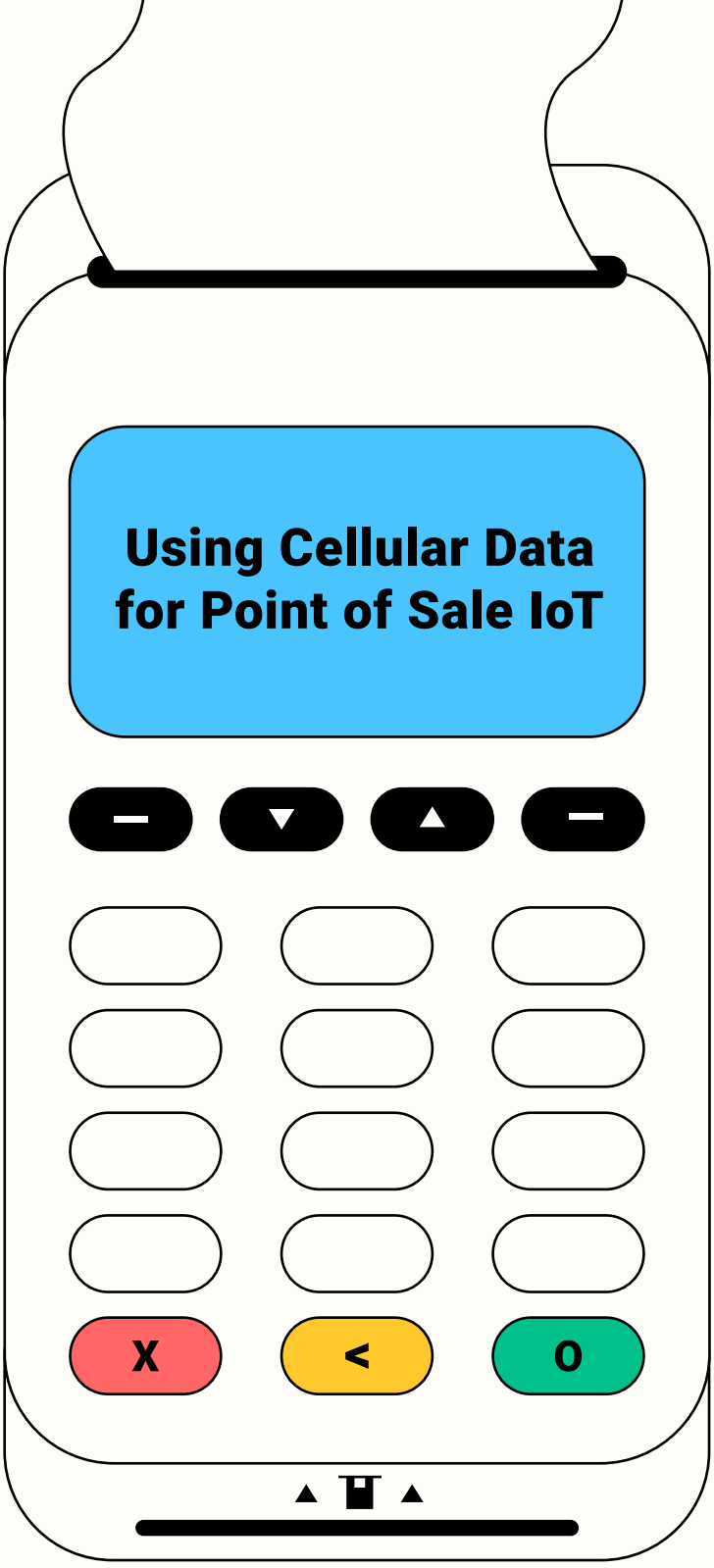


Telnyx helps you weigh the pros and cons of cellular data vs WiFi as it applies to Point of Sale IoT devices.

What's inside

IoT today

The Internet of Things (IoT) has fundamentally changed the way we interact with our devices, powering novel experiences for consumers, streamlined processes and costs for businesses, and new economies for manufacturers worldwide.

As we approach 2023, Statista projects global spending on IoT will hit $1.1 trillion[1]. Not only is IoT a global economic driver: it's transforming our behaviors and decision-making processes.

$1.1 trillion

is the predicted amount global spending will reach for IoT in 2023.

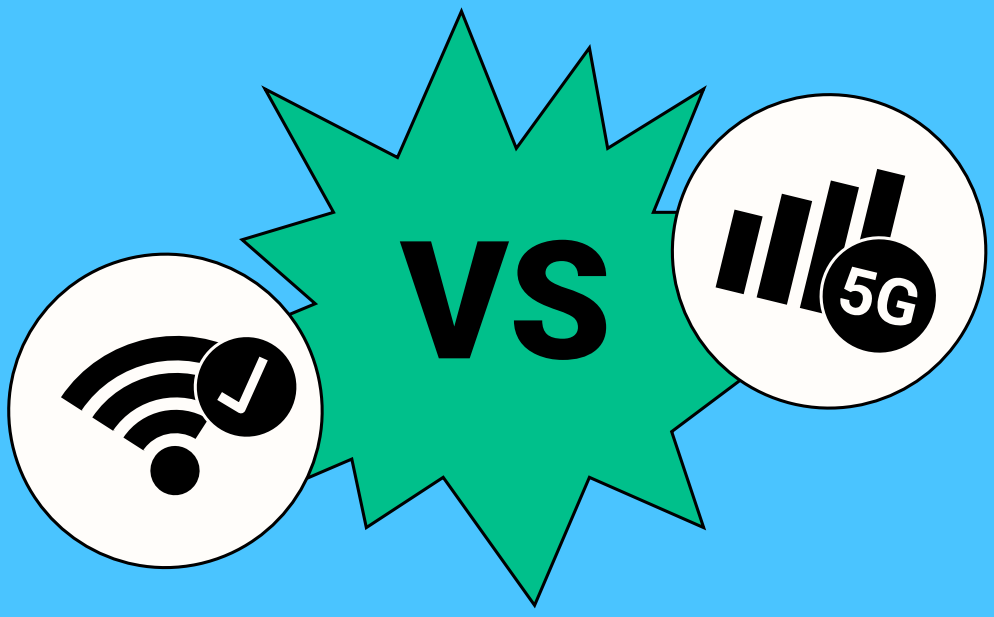
As Forbes predicted in 2014, "The new rule for the future is going to be: anything that can be connected, will be connected."[2] With an estimated 14.4 billion active IoT devices today[3], the use cases for IoT technology are only expanding. From wearable technology and smart home devices, to vehicle fleet management systems and on-site track-and-trace monitors, IoT systems are proliferating at every level of human activity.

14.4 billion

is the estimated amount of active IoT devices today.

As we become more dependent on IoT, a question arises:

How do we ensure these devices stay connected and functional?



IoT connectivity: WiFi vs. cellular

As their name implies, IoT devices depend on stable, secure internet connections to function. The two most popular wireless technologies for IoT networking are WiFi and cellular data.

IoT devices have historically been powered by WiFi. Take smart home devices—one of the earliest popularizations of IoT—for example; WiFi has been the dominant internet connectivity method for smart home products, and continues to be today. So, IoT devices intended for usage in spaces with WiFi access (like shops, malls, or restaurants) have often received the same treatment as smart home devices—why bother giving a device its own data connection when there's a WiFi network up and running?

What's more, cellular networking didn't exactly deliver on accessibility a decade ago. Cellular data was expensive, with less accessible hardware and inconsistent coverage. In recent years, cell data coverage has expanded, prices have decreased, and SIM card production has diversified, making cellular data more obtainable.

39%

of the total wireless infrastructure revenue in 2021 was dominated by 5G as the fastest growing segment in wireless network infrastructure, according to Gartner. This is a result of the COVID-19 pandemic, which "spiked demand for optimized and ultrafast broadband connectivity to support work-from-home and bandwidth-hungry applications, such as streaming video, online gaming and social media applications."[4]

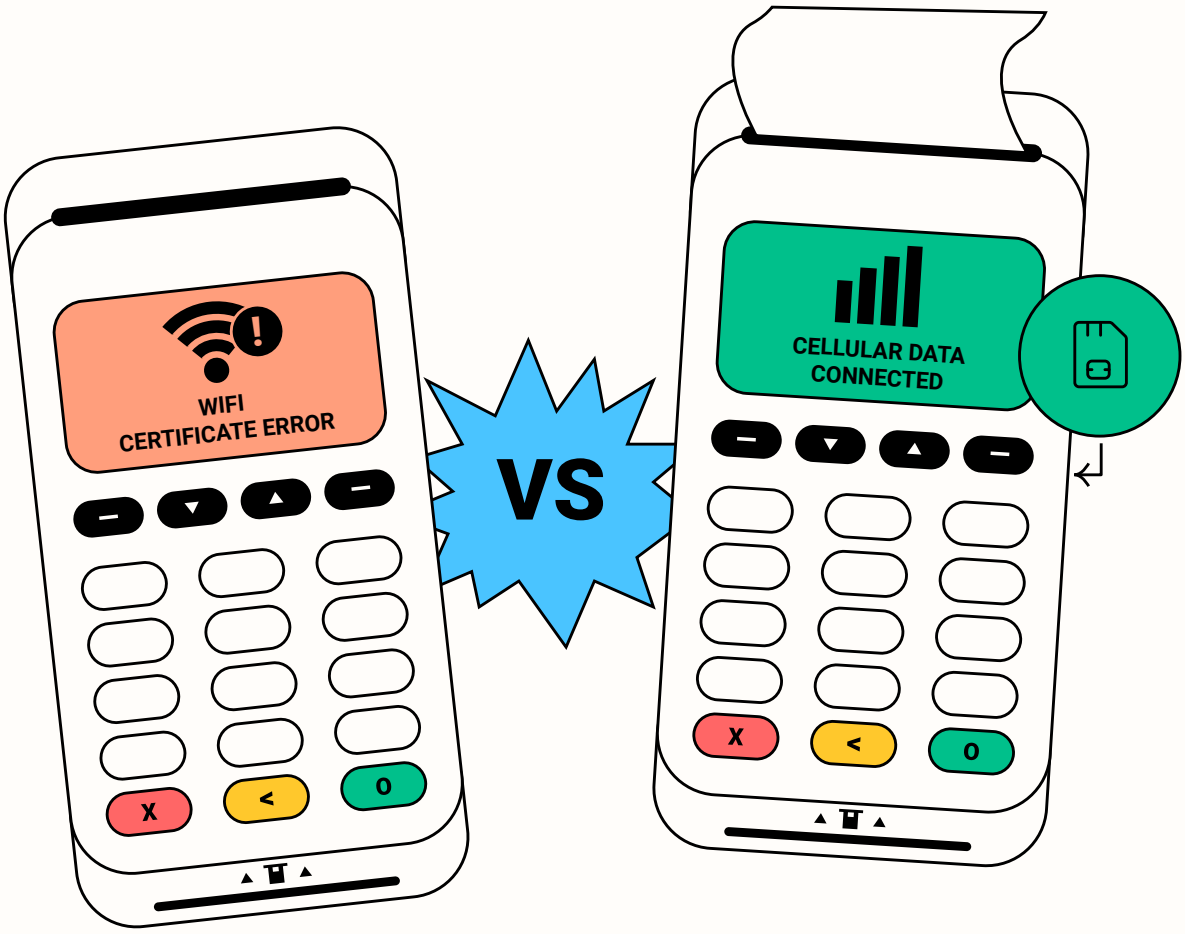
With faster, more accessible cellular networks available globally, cell data is an increasingly preferable connectivity method for IoT devices. To compare these options, we examine four main criteria: configurability, coverage, security, and bandwidth—and cell data proves to work best for building IoT applications across the board.

1

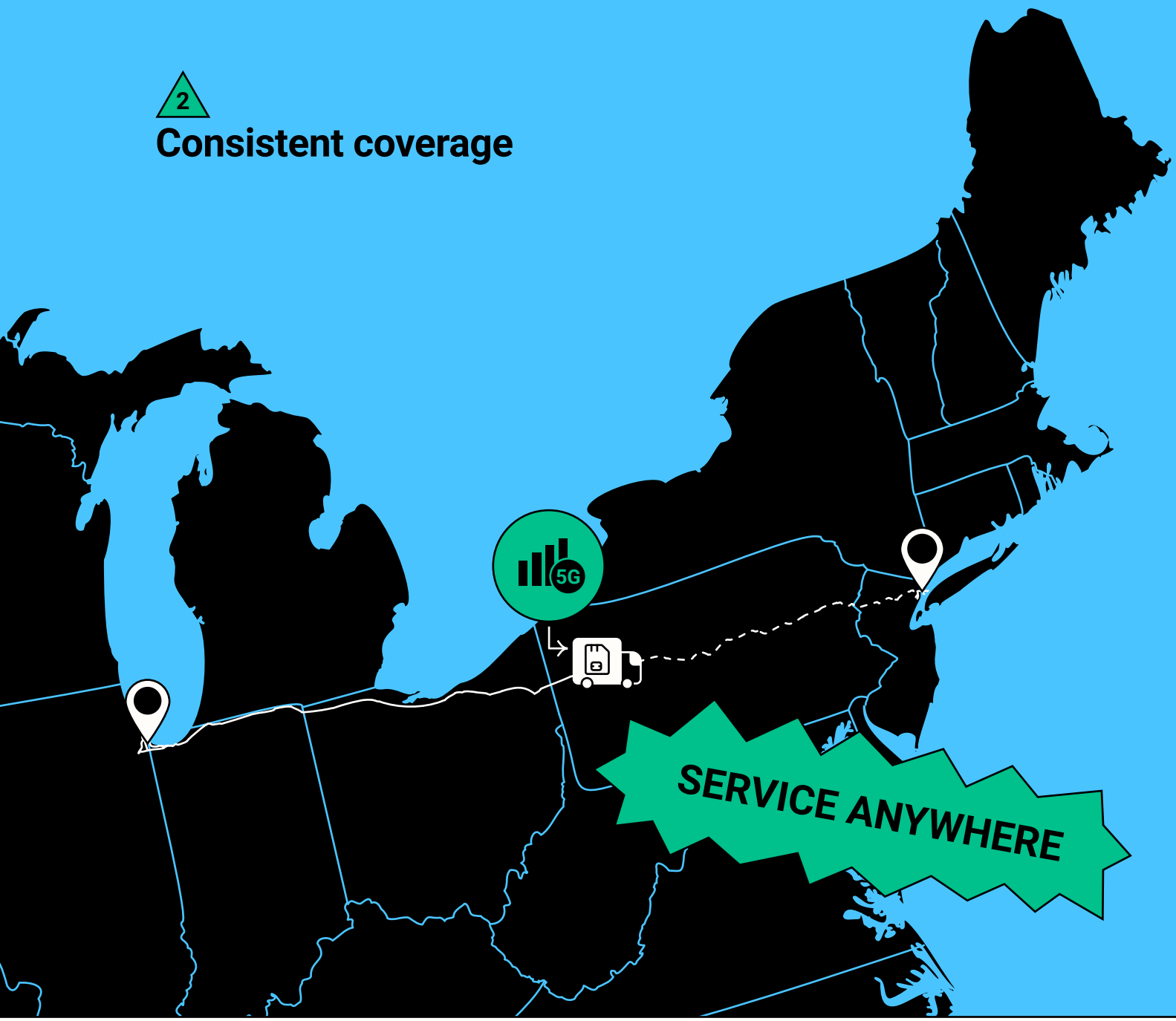
Easy setup and configuration

Activating cellular data on an IoT device is as simple as ordering a SIM card and placing it inside your device. With WiFi, configuration is more complex as it involves connecting larger sets of hardware (routers, modems, etc.) and higher dependencies on your internet service provider (ISP).

Deploying IoT devices in corporate or franchise environments requires working with IT departments—often remotely—to get the WiFi up and running, which can be slow and frustrating. Even if your IoT deployments are better suited for WiFi, cellular data can still play a critical role in your platform uptime and resilience. Ensuring that devices are fitted with SIMs allows cellular data to act as a fall-back when WiFi networks falter or crash.



2
Consistent coverage



WiFi usually operates as a local area networks (LAN) so users may experience dropouts as devices move away from their dedicated area. In contrast, cell data providers continously invest in infrastructure that enhances network coverage and speed, forming a wide area network (WAN) and making cellular data stronger, faster, and more reliable.

When it comes to deploying IoT devices outdoors, in remote areas, or in transit, cellular data is the only option for devices that require a constant flow of communication.

Strong security

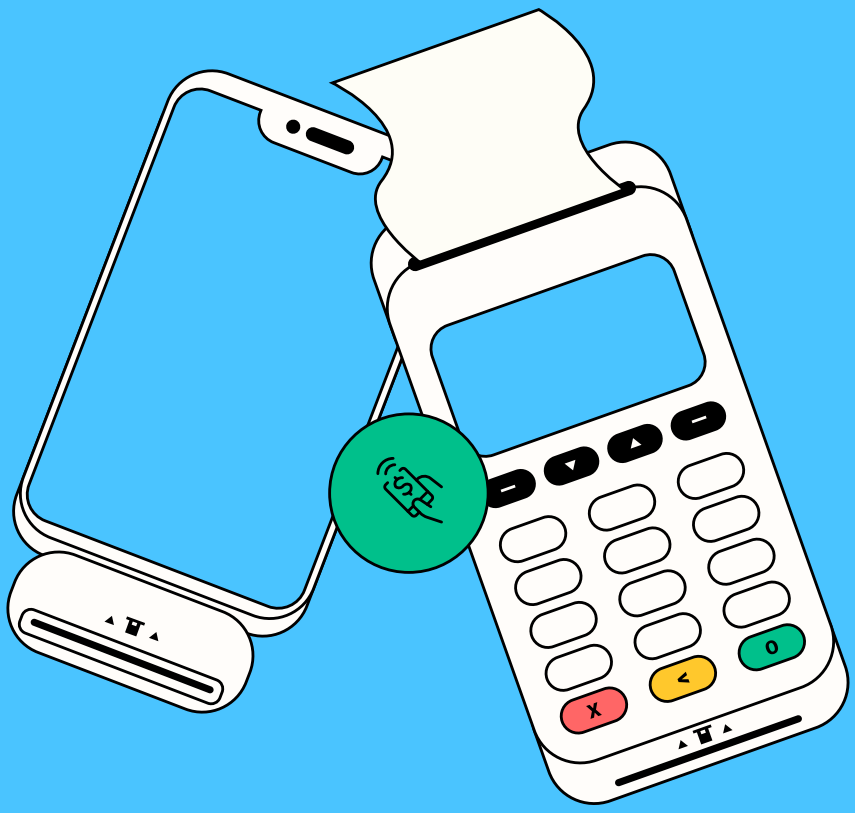
Connecting to the internet through cellular data is empirically more secure than WiFi. Not only is cell data encrypted under typical circumstances[5], network providers prioritize cellular security. Operators have teams of experts maintaining the security of their platforms, data, and accounts through vigilant monitoring and regular updates. These businesses have a vested interest in maintaining safeguards because they face fiscal and reputational repercussions if security is compromised.

On the other hand, the security of WiFi networks is based on the individual network owner. Most WiFi owners aren't well-versed in cybersecurity practices like data encryption or regular network security updates. In addition WiFi networks are vulnerable to popular cybercriminal activities. A common attack—also known as a "man-in-the-middle" attack—involves setting up fake WiFi networks in the vicinity of a valid network[6]. Unsuspecting device owners join this network and when devices are processing payments or sensitive data through that network, the data becomes vulnerable.

High bandwidth

The development and proliferation of 4G+ networks have leveled out the playing field between WiFi and cellular data bandwidth. For years, WiFi's 450 megabits per second (Gbps) standard and more recently, its ability to reach 1.3 Gbps makes it superior in speed. However, 4G LTE is catching up to WiFi speeds with a standard of 1Gbps. With new promises of WiFi based on the 802.11ax (also known as Wi-Fi 6) standard reaching speeds up to 10Gbps, new cellular technologies will place 5G at similar speeds. Today's cellular networks have closed the bandwidth gap, making the two technologies equally capable of high-speed connectivity.[7]

With the advantages of cellular-enabled IoT connectivity in mind, let's dive into one of the most prevalent applications of IoT technology: Point of Sale.



IoT for in-store payments

The COVID-19 pandemic has transformed the way we shop.

With 75% of Americans trying new shopping methods during this period and consumers switching brands at unprecedented rates[8], retailers are under pressure to convey value and deliver positive customer experiences—regardless of where they're making sales.

In any retail experience, payments are a constant—but optionality has never been higher. Today's e-commerce retailers offer multiple payment solutions, particularly interest-free installation programs through Paypal Credit, Afterpay, Klarna, and the like. In physical stores, connected payment experiences powered by innovative technology like Amazon's "Just Walk Out" technology[9] are changing our conception of what it means to pay for your goods.

75% of Americans tried new shopping methods during the pandemic and consumers switched brands at unprecedented rates.

Point of Sale devices

In this day and age, the very least brick-and-mortar retailers can offer are modern, mobile payment terminals that customers can tap or swipe quickly from wherever they are in a store. These devices are categorized either as Point of Sale (PoS) or Mobile Point of Sale (mPOS).

Mobile Point of Sale

Mobile Point of Sale (mPOS) enables businesses to use phones and tablets to complete payment transactions through a downloadable app. By using these devices to process payments, mPOS allows businesses to streamline equipment and optimize customer service. mPOS has gained serious traction in the retail industry—as of 2020, adopting an mPoS system remained a priority for 44% of large North American retailers[10].

44% of large North American retailers prioritized adopting a mPOS system in 2020.

Despite its perceived conveniences, mPOS is not the be-all-end-all brick-and-mortar payment solution—it has serious risks and disadvantages when it comes to security. While PoS devices operate on a closed payments processing system, mPOS systems are only as secure as the commercial off-the-shelf devices they operate on, and the downloadable app they use to process payments. To that end, a hacker who penetrates your payment processing app can potentially access transaction data, including customers' card details. Needless to say, the potential fiscal, legal, and reputational consequences of hosting poorly secured payment systems are serious. In today's hypercompetitive retail environment, insufficient security is not something brands can afford.

Point of Sale

In contrast, dedicated PoS devices provide a closed-loop payment processing system, designed for hardware and software security. These devices, available as either handheld or counter-top, provide the same seamless checkout process and flexibility of an mPOS system, with far fewer vulnerabilities.

The main challenge for dedicated PoS devices is consistent connectivity, and with the right provider that challenge is easily solved. With multi-carrier SIM cards, PoS devices can switch between networks automatically to ensure consistent, cost-effective coverage.

Mobile Point of Sale (mPOS)

(+) Use existing device

(+) App to process payment

(-) Security risks

Point of Sale (POS)

(+) Closed-loop processing

(+) Handheld or countertop devices

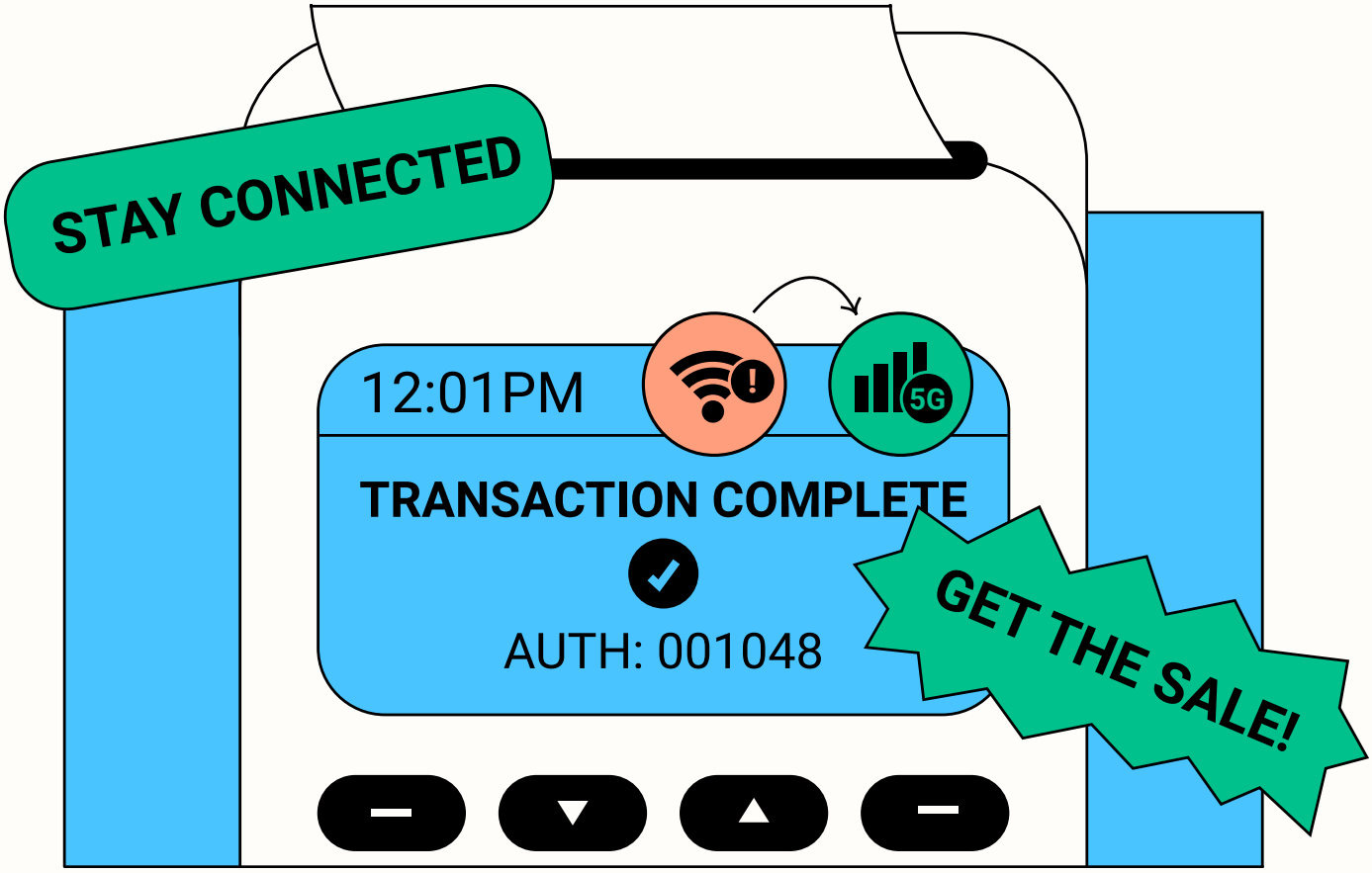
(-) Needs consistent connectivity

PoS device production

PoS device vendors operate at various points of the production line. Some manufacturers focus purely on hardware, offering payment terminals complete with cellular data and/or WiFi functionality, but without a network connection. Other PoS providers offer ready-to-use devices, buying hardware from vendors and reselling them to retailers as part of a managed services package that includes data connectivity.

Cellular data fall-back functionality is the minimum

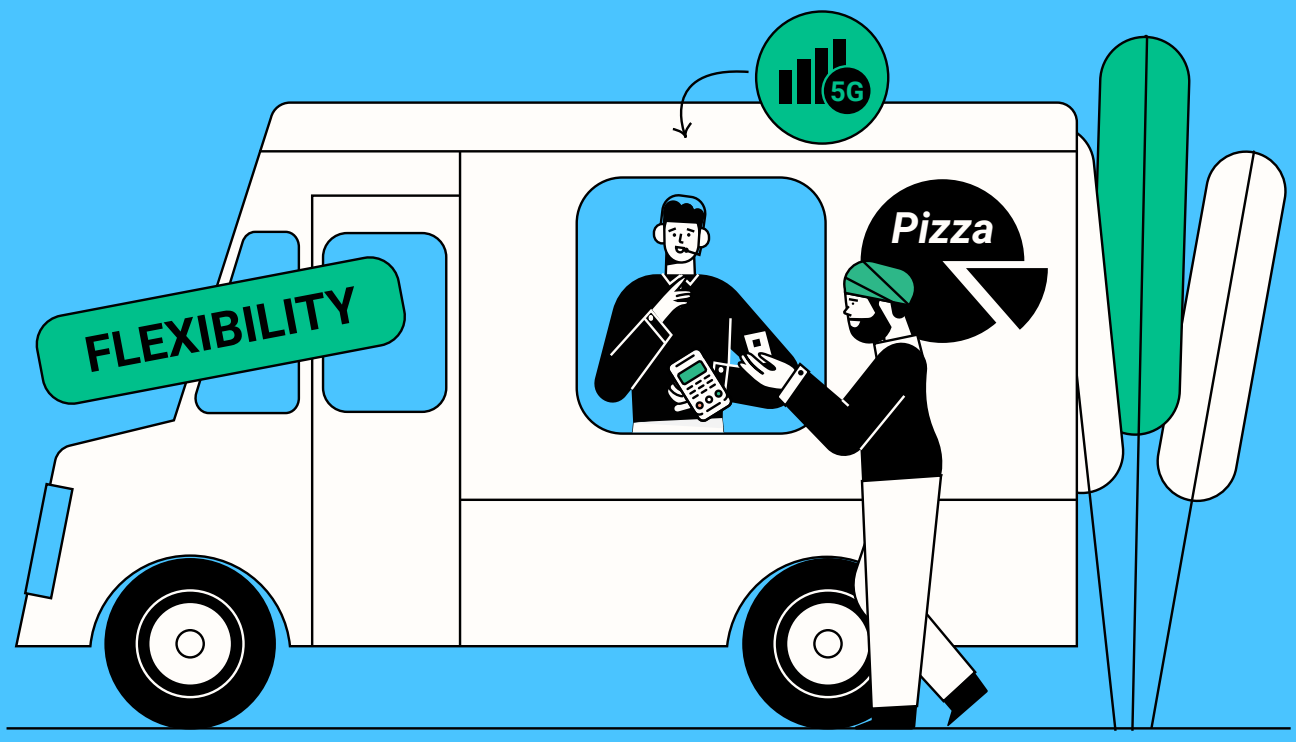
Stable, broad internet coverage within a brick-and-mortar store is essential for PoS systems to process payments correctly. The last thing retailers want is prolonged or failed transactions that give shoppers time to second-guess their purchases. If an internet outage occurs and a payment system loses its internet connection, shops run the risk of missed or incorrectly processed transactions. This can result in lost business or accidental free handouts.



With these consequences at stake, PoS vendors often sell devices or solutions with fall-back cellular data connectivity. The reality is WiFi connectivity is never fully reliable. Ever wait on a slow payment system at a coffee shop when you're ready to pay and go? Ever been unable to make a purchase at a boutique because the payment device isn't connecting to the internet? Ever struck up a conversation with a cashier because the terminal is taking ages to confirm your payment? These payment systems likely operate on a WiFi connection, without cellular data backup. By making this simple adjustment, retailers can fortify their transactions.

Take franchises for example. Brick-and-mortar franchises often have to deal with corporate internet setup processes and troubleshooting protocols. The complexities of connecting to corporate WiFi networks can be cumbersome and error-prone, resulting in added strain on franchise staff and IT teams. Cellular data offers a simpler alternative.

Mobile retailers stand to benefit more from cellular data-powered PoS systems. Food trucks, farmers' market stalls, and pop-up shops appeal to customers with their unique offerings, distinctive shopping experiences, and limited availability. But in order to capitalize on their niche, mobile retailers depend on convenient, reliable payment processing systems. While these shopping experiences are rarely situated near a stable WiFi source, cellular connectivity offers total flexibility and peace of mind.



What PoS device vendors should look for in a SIM card provider

Fitting PoS devices with SIM cards is critical for vendors looking to provide competitive, reliable products at scale. But not every SIM card is created equal. Below, we highlight key features PoS device vendors should consider when choosing a SIM card provider.

- **Per megabyte, pay-as-you-go pricing**
- **Standby mode**
- **Multi-tenant SIMs**
- **In-house telecommunications expertise**
- **A suite of communications tools to complement payment processing**

PER MEGABYTE, PAY-AS-YOU-GO PRICING

A single transaction generally uses around 10kb of data, but many SIM providers only offer package pricing. For most businesses, paying hundreds of dollars a month for a huge data allowance is money wasted—especially if your customers' sales, like most retailers, fluctuate seasonally.

STANDBY MODE

Stocking ready-to-use PoS devices allows for shortened sales cycles and faster order fulfillments, resulting in faster business growth and happier customers. But many SIM card providers don't offer functionality for programmatic, remote SIM activation with low-cost standby mode. When evaluating providers, make sure you avoid high monthly fees before your SIMs are in use, and select a provider that delivers a seamless activation process once devices turn on.

MULTI-TENANT SIMS

Spotty connectivity results in declined payments, missed sales, and frustrated customers. Even if a PoS device is capable of processing payments in “offline mode”, your customers stand to lose revenue. Let’s say a shopper uses their card to buy an item. They leave with their new purchase while the offline payment terminal stores the transaction data in-cache. Later, when the PoS device is back online, it processes the payment, only to relay that the card has been declined. Now, your merchant has handed out free product at their own expense.

Fortunately, PoS device vendors can minimize network dependencies with multi-tenant SIMs. These SIMs are able to connect to multiple major carriers so coverage never drops. More advanced models will intelligently measure signal strength and switch to the network with the best coverage. By fitting your PoS devices with intelligent multi-tenant SIMs, you can optimize transaction speed and empower customers to deliver seamless experiences.

Multi-tenant SIMs are also critical to international expansion, which, for a PoS device vendor, is likely inevitable. Whether you’re scaling your business independently or in support of existing customers, international network coverage is essential. But working with network operators on a per-country basis is taxing—both in setting up partnerships and in maintaining them. Individual operator partnerships can create situations where you’re managing different devices with different SKUs and SIM cards for every country you’re operating in. Instead, look for one global SIM card with multi-tenant coverage in the countries you’re operating in or want to expand into.

IN-HOUSE TELECOMMUNICATIONS EXPERTISE

Running apps that rely on cellular connectivity at scale gets complicated quickly—international regulations and carrier relations can get increasingly difficult to navigate. A provider with proven telecommunications expertise and a history of successfully onboarded PoS customers will be more able to support and advise you on effective SIM deployment. By leaving complex networking and regulatory work to an expert partner, you’re able to build things right the first time around, and focus on scaling efficiently.

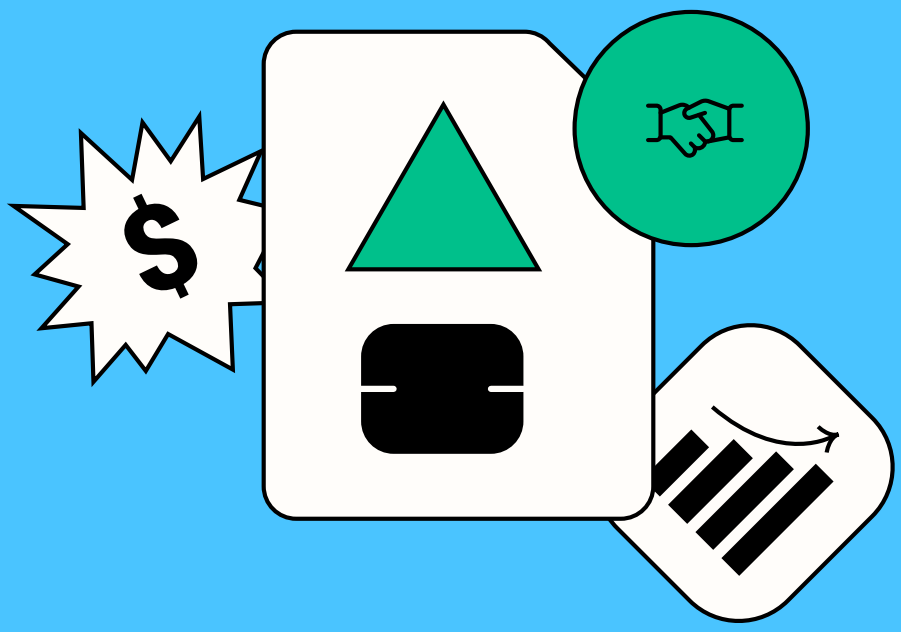
A SUITE OF COMMUNICATIONS TOOLS TO COMPLEMENT PAYMENT PROCESSING

PoS vendors are strengthening customer relationships by offering more than payment processing services. Customer engagement and support solutions can become part of your arsenal with very little legwork. All it takes is partnering with a connectivity provider that offers communications solutions across messaging, voice, and other popular channels.

The applications of combined payment and communications solutions are expansive. You can:

- Enable your customers to send transaction receipts to customers via SMS.
- Add a consent tick-box on your receipts so merchants can send customers personalized offers.
- Use SMS receipts so merchants can link customer records to purchasing activity.

By providing communication tools in conjunction with a payment solution, you empower your customers to better understand their shoppers and deliver integrated shopping experiences.



Partner with a cellular data provider that scales with you

As a PoS vendor, you may want to enter new global markets and service new industries. With the right connectivity infrastructure in place, you'll only have to focus on serving your new and existing customers.

When evaluating your PoS device connectivity, make sure your devices are SIM-friendly, so you can fit the devices with multi-tenant SIM cards that offer reliable global connectivity, programmatic configuration, and fair pricing.

Telnyx Wireless

Telnyx Wireless offers multi-tenant SIM cards that leverage 400+ global carrier connections and coverage in 180+ countries, along with an API to manage and monitor SIMs remotely and programmatically. With standby-mode, pay-as-you-go, per-megabyte billing, and zone-based pricing, we power efficient data coverage at scale. Our suite of CPaaS tools is ready to use when you're set to expand your offering.

400+
global carrier connections

180+
countries with coverage

API
to manage and monitor SIMs

Ready to build the next generation of Point of Sale IoT devices?

Contact a member of our team today

Telnyx is a software-driven connectivity company designed for the future.

Telnyx is a global connectivity platform and partner that provides carrier-grade services on a private, cloud-agnostic IP network. Our Voice, Messaging, Numbering, Video, Wireless, Fax, and Security solutions are accessible through RESTful APIs and our award-winning Mission Control Portal.

Telnyx is a licensed carrier in over 30 countries. Cutting out the middleman allows us to drive efficiencies, provide better products to our customers, and set industry standards for price, value, and quality. From in-app messaging and calling to feature-rich contact centers to IoT networking solutions, Telnyx solves connectivity needs at every complexity level, with 24/7 in-house engineering support on hand.

Founded in 2009 with offices in Chicago, Dublin, Amsterdam, Warsaw, and São Paolo, Telnyx delivers mission-critical communications for customers including Cisco, Philips, Slack, Red Cross, and more.

1 Statista, Internet of Things (IoT) - statistics & facts, May 11, 2021.

2 Forbes, A Simple Explanation of The Internet of Things, May 13, 2014.

3 IoT Analytics, State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally, May 18, 2022.

4 Gartner, Gartner Forecasts Worldwide 5G Network Infrastructure Revenue to Grow 39% in 2021, August 4, 2021.

5 New York Times, The Security of Cellular Connections, August 10, 2018.

6 Vice, How a Wi-Fi Pineapple Can Steal Your Data (And How to Protect Yourself From It), November 20, 2017.

7 Tech Target, Battle of the IoT networks: Cellular versus Wi-Fi, April 25, 2018.

8 McKinsey, The great consumer shift: Ten charts that show how US shopping behavior is changing, August 4, 2020.

9 Forbes, 5 reasons why Amazon Go is already the greatest retail innovation of the next 30 years, March 1, 2022.

10 Digital Transactions, 2020 POS/Customer Engagement Survey from Retail Consulting Partners.


TELNYX