TEAM Software

Indoor Location Technologies Compared

AN EBOOK FROM TEAM SOFTWARE

Whether your goal is stronger customer engagement, improved productivity or risk mitigation, cleaning and security businesses need accurate indoor location information. But which technology should you use — Bluetooth Low Energy (BLE) beacons, GPS, Wi-Fi, radio-frequency identification (RFID) or near-field communication (NFC)? In this eBook, find out how and when to select one technology over the other.

TABLE OF CONTENTS

CHAPTER

01

OVERVIEW

INTRODUCTION

Businesses with distributed workforces, like security and cleaning contractors, need indoor location information to be accessible and cost effective. GPS, BLE beacons, Wi-Fi, RFID and NFC are all important pieces of the puzzle, but each has its advantages and limitations.

Because trust is at the heart of cleaning and security services, your guard touring and location tracking software should enable real-time visibility of your entire workforce and provide assurance that all tours, loops and tasks are completed. Whether you're a security contractor tracking guard tours and patrols, or you're a cleaning contractor who monitors loop times and rotations, touring and tracking software helps you improve performance, reduce costs, prove service and mitigate risk.

So, which tracking technology should your business use? Unfortunately, no single solution is the perfect answer to all problems. Usually, the right answer depends on what you're trying to achieve, your environment and your budget.

lighthouse
powered by TEAM Software

Using a mobile workforce management solution like Lighthouse ensures your guards and cleaners are where they're supposed to be. And, you can provide your customers with proof of work to increase satisfaction.

To help you navigate the indoor location tracking landscape, we're comparing the five most talked-about location tracking technologies: BLE beacons, Wi-Fi, RFID, NFC and GPS. Because this is a complex topic, it's hard to draw exact apples-to-apples comparisons. That said, the goals of this guide are to:

1. Discuss the major factors and tradeoffs for evaluating indoor location tracking technologies.

2. Provide basic parameters for the average buyer to help narrow down options and focus their search.

EVALUATION FACTORS

In a perfect world, we want a universally accessible location system that's highly accurate, secure and cost-effective. We're using the following attributes to assess each technology.

Accessibility

Accessibility refers to technology's ability to be tapped into or accessed by a consumer or business. Regardless of the technology type, determining location always requires some type of infrastructure: a sender (or transmitter), a receiver and a data service. Some systems require additional antennae or translators for value-add functions. For example, to report precise room positioning, RFID systems supplement zonal readers with active RFID rack room locators.

The more universal those senders and receivers are, the more accessible the system. For example, GPS is a highly accessible technology because there's a single global standard for transmitters (satellites built by the U.S. government) and nearly all mobile devices can act as receivers.

Range

Range refers to the distance the signal travels. For the solutions in this eBook, range can depend on the configuration, power settings and environment. For example, a Wi-Fi or Bluetooth signal travels much farther outdoors without any obstruction than in a multi-room, multi-surface indoor setting. Additionally, it's possible to turn up the power to project a longer-distance signal. This is often the case with Wi-Fi, since the requirement for power and internet generally means fewer access points over longer range is preferred.

Accuracy

Accuracy refers to the reliability of the signal within a given range, and the tolerance of that signal when accounting for environmental factors. For example, beacons are typically more accurate indoors than Wi-Fi because the portable nature of the beacon transmitters allow for configuration workarounds that account for signal refraction and poor reception zones.

Security

Security refers to the ability of data sent over the system to be hacked or accessed by third parties or malicious intruders. We discuss privacy along with security for simplicity.

Cost

Cost includes the expense of setting up, using and maintaining the systems. While cost effectiveness is often relative to the situation, cheaper is typically better when calculating ROI.

SO HOW DO THEY STACK UP?

The table on the next page summarizes the performance of each technology solution against these variables. For comparison purposes, we used a 1-5 scale with every technology starting at a perfect 5 and deducted a point for each major drawback or limitation.

Note: we've included signal range in the table but haven't assigned it a rating. In some scenarios, a completely global range is best but in others, restricting to a specific area is required.

	Beacons	GPS	Wi-Fi	RFID	NFC
How it works	Bluetooth Low Energy beacons send a signal; device detects signal and acts based on data service rules	Satellite radio signals; GPS devices receive the signal and determine location	Wireless access points detect devices and triangulate based on received signal strength	Radio tags transmit stored information (passive or active) to readers which record data and/ or perform actions based on reader application software rules	Passive UHF RFID chips (usually built into a device or card) transmit data to terminals upon close contact
Typical Range	3-160 feet	Unlimited	65-160 feet	Less than an inch to 3 feet	4 inches or less
Accessibility (network infrastructure required)	4	4	3	2	3
Accuracy	4	1	3	5	5 (near-range only)
Privacy and Security	3	3	2	4	4.5
Cost	4	5	3	2	3
Best for	Indoor tracking; passive notification of contextual information; peer-to-peer messaging	Outdoor tracking and navigation; agriculture and military use	Existing infrastructure and/or strong need for Wi-Fi connection and location information accuracy is only required within meters	SKU level tracking of inventory, requirements for less than an inch accuracy	One-to-one secure delivery of information between consumer and another entity (payment ticketing, etc.)

THE DETAILS

As you can see, there isn't a clear winner; it depends on the application of the technology. In many cases, the best solution for your security or cleaning business is a combination of techniques. To select the best option for a given use case, you must consider the influencing factors and requirements (i.e., tracking accuracy, budget/ infrastructure, security, etc.). In the following chapters, we go into a more detailed explanation of each location system against our evaluation criteria.

CHAPTER

02

BEACONS

Bluetooth Low Energy (BLE) beacon-based location systems are built to respond to existing weaknesses in indoor positioning and proximity services. Beacons are an agile and portable solution for people and asset tracking and communication.

HOW IT WORKS

Small wireless devices called beacons broadcast signals using BLE, a power-friendly version of traditional Bluetooth. Nearby smart devices listen for these signals, trigger actions and/or record analytics via mobile apps based on device proximity.

Beacon facts

- Based on BLE
- Available in different formats, including small coin cell powered devices, USB sticks and software versions built into other devices (e.g. light-bulbs, vending machines, etc.)
- Supported by most Apple smart devices as well as Android devices with Android 4.3 or later
- BLE uses 2-3% of a phone's battery — significantly less than Wi-Fi would consume over the same period.

lighthouse
powered by TEAM Software

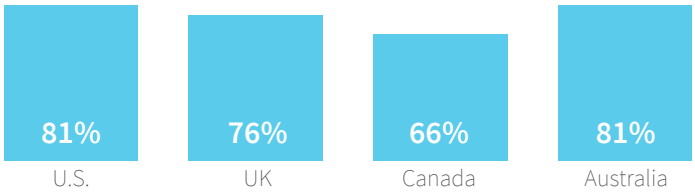
When your customers question if a patrol or loop was completed, you can rely on a workforce management solution like Lighthouse to pinpoint exactly where a guard or cleaner is and where they've been through real-time and back-in-time reporting thanks to beacon technology.

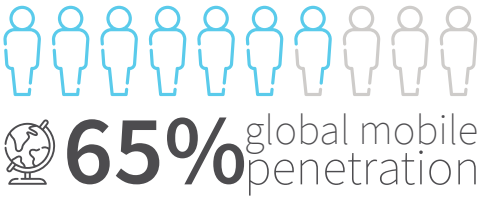
ACCESSIBILITY: MEDIUM - HIGH (4)

Beacons are the signal transmitters (senders) in a BLE location system. They're battery-powered, stick to almost any surface and can be configured from a mobile app, making them scalable and highly portable. And, since they operate on a low energy form of Bluetooth, a single device can last one to three years. However, unlike a universal system like GPS, installation of these transmitters is required and also requires maintenance to replace batteries or beacons. (-1)

A benefit of beacon systems is they primarily use mobile devices as the receiver system. And, because smart devices and cellular networks have become essentially universal (even in remote areas and developing countries), the receiver network is highly accessible. Because a mobile app is required, for a beacon system to achieve high penetration, the value proposition to download an app and turn on location services must be high.

Smart phone ownership by country:





Source: Pew Research Center

ACCURACY: HIGH (4)

Beacons operate on the 2.4 gigahertz frequency which is also the most commonly used Wi-Fi frequency. Like all radio signals at high frequencies, reliability of Bluetooth signals is impacted by the environment. However, since the beacon system is highly flexible, issues of line of sight (LOS) and signal reception that impede Wi-Fi and GPS accuracy indoors can all be addressed by freely altering the Bluetooth beacon network, either by manipulating the individual beacons or simply adding more.

Beacons are generally known as a proximity service, meaning they sense when another device is in range. Beacon ranges can be configured to project from approximately 10 to 160 feet. It's also possible to achieve accuracy as low as three feet using a range of techniques (e.g. signal ranging, location fingerprinting or trilateration).

SECURITY: MEDIUM - HIGH (3)

Since BLE beacons broadcast outbound signals, there's no inherent security risk embodied in the transmission. The risk lies primarily in the apps that use these signals. In this sense, beacons are no better or worse than any other location service communicating via a mobile device. However, systems like NFC that enable secured sessions emulating the way contactless cards (e.g. credit cards, ID cards, etc.) transmit data are generally considered more secure for things like payments. (-1)

One threat to beacon security is often referred to as beacon hacking. Beacons with weak security measures can be discovered by hackers in public places and have their universally unique identifier (UUID) Majors and Minors changed. Some manufacturers have put measures in place to prevent this from happening but, depending on the beacon manufacturer and their built-in security, it may still be a risk. (-0.5)

Another criticism of beacon systems is piggybacking. This occurs when a third party discovers your beacon UUIDs, and then leverages your beacon network without permission. Many beacon providers now provide UUID scrambling to prevent this from occurring, though it remains a weakness in less sophisticated deployments. (-0.5)

Compared to some of the other options, beacons win points on privacy. Unlike Wi-Fi, which detects an individual's presence without opt-in, beacon systems allow the user to control their settings by turning Bluetooth and location services on or off. And, permission gates are in place to ask the user as they download the app. Businesses are forced to make a compelling case to consumers and employees for turning on tracking capabilities. One common misconception is that beacons themselves track and store smart device location. In reality, most beacons only broadcast an outbound signal and don't receive or store any additional information.

COST - LOW (4)

The main costs associated with a beacon system are the beacon hardware (including the cost of deployment), the licensing / data service costs and the receivers or devices.

Beacons themselves are relatively cheap. You can typically find beacons from $5-$30 each depending on volume. The number of beacons used depends on the size of the space and range required. For a business, it's more expensive than GPS, but less than RFID readers or Wi-Fi access points. (-1)

Receivers or device costs depend on the use case. This is generally free as it's just using existing personal smart devices. For enterprise cases, a business may prefer to supply a device to employees. Basic, no-frills smart devices can start at $50 per unit and go up from there.

Other costs not considered in this analysis are any fees associated with a custom mobile app, integration with other systems and licensing. App and integration costs depend on the use. Licensing fees are typically dependent on the volume of interactions being processed.

VERDICT

Beacons may be the newer kid on the block, but as long as there's a clear value proposition for an app, it's the best option for indoor location positioning, communication and analytics. The combination of flexibility, accuracy and a low-cost infrastructure edges out Wi-Fi and RFID. In addition, the opportunity to seamlessly integrate with existing and new mobility applications greatly improves its benefit to businesses. However, for outdoor uses, secure payments or SKU-level tracking, other systems like GPS, NFC or RFID may be needed to complement a beacon system.

CHAPTER

03

WI-FI

Wi-Fi based positioning systems are commonly used to overcome the inadequacies of GPS indoors. They have the advantage of also providing a value-add service (internet access) and, therefore, are a pre-existing infrastructure in many establishments. Many companies have developed systems that allow for some navigation and indoor location analytics using Wi-Fi.

HOW IT WORKS

Wi-Fi hot-spots are effectively fixed anchor points providing a static known position. A device detects a Wi-Fi access point and, once multiple points are detected, can determine its position. Wi-Fi implementations require access points, a data service that computes location (and keeps track of all the locations at any given point), and a location-specific context (a blueprint overlay of the building).

ACCESSIBILITY: MEDIUM (3)

The Wi-Fi receiver infrastructure is relatively universal as it works well with mobile devices and doesn't require you to sign into the Wi-Fi network or opt-in to location services to work for tracking purposes. However, while tracking location may not require an app, like other systems, moving beyond tracking to communicate does require a communication interface and opt-in, like an app. (-1)

Additionally, the requirement of internet access, power points and software to identify the various Wi-Fi networks makes the infrastructure relatively difficult to set-up. While this may be feasible at major shopping malls and department stores, it may be cost prohibitive to extend to other, smaller locations. (-1)

ACCURACY: MEDIUM (3)

Existing Wi-Fi access points may be unreliable, inconvenient and poorly placed for the situation at hand. The fixed nature of Wi-Fi access points and relatively high cost of installing them means there's limited flexibility in altering the network and it's difficult to achieve the level of precision afforded by beacons or RFID. (-1)

Additionally, Wi-Fi systems' ability to identify individuals for navigation and analytics is limited, particularly by Apple devices. For your phone to detect a Wi-Fi network, it sends out a string of data that's unique to your phone. Retailers use Wi-Fi sniffers to listen for your phones unique signature and, thus can tell you're in the vicinity. A Wi-Fi sniffer is a portable tool for locating the nearest wireless connection. It will also help you to determine the strength of the Wi-Fi signal and if there are multiple signals, and will prioritize the signals in terms of strength which saves the user time and frustration. Previously, these signatures were static and so Wi-Fi could identify unique users. However, due to changes in the technology, now businesses may be able to detect a device, but they can't necessarily tell if the device is unique. (-1)

SECURITY: MEDIUM (3)

Unlike GPS or BLE, data is being transferred over a Wi-Fi network, meaning hacking into the network poses more of a risk than its counterparts. Wi-Fi has adopted various encryption technologies to secure the network and the technology has come a long way over the years. Security depends on the encryption techniques used and there are a lot of companies out there that specialize in providing secure wireless connections and data exchange. (-2)

COSTS: MEDIUM (3)

If there's an existing Wi-Fi network in place and location details are only needed at the room or zone level, Wi-Fi can be a great, low cost solution. However, if location information is needed at a high-level of accuracy or movement needs to be recorded, the number of access points and data service required becomes more complex and more expensive. (-2)

Other costs associated with Wi-Fi location systems include internet charges, maintenance and an app for users to download so the positioning has the correct context and protocols.

VERDICT

The verdict for Wi-Fi depends on the level of precision and existing infrastructure. Wi-Fi has a much higher bandwidth, so when internet access and data transfer is required, it's a critical solution component. However, for accurate indoor location analytics, user positioning or tracking, beacons and RFID are both better solutions.

CHAPTER

04

RFID

Radio frequency identification, commonly known as RFID, is a form of wireless communication that uses radio waves to identify and track objects. RFID takes the barcoding concept and extends it with more three-dimensional information and active tracking capabilities. It's a hugely popular system in distribution, logistics and inventory management for the ability to identify many items at once without direct line of sight.

HOW IT WORKS

An RFID system is comprised of tags, readers that communicate with each other using radio waves, and reader control and application software. RFID systems are broadly categorized as Passive or Active. Passive systems are characterized by tags that are powered by the readers, meaning they don't require a power source. Active systems have more expensive, battery powered tags that broadcast their own signal up to 300 feet.

There's wide variability in the cost and functions of RFID systems based on the different types of tags and readers. We can't cover all variables within an RFID solution, but we discuss the main variables and trade-offs.

Tags

An RFID tag is comprised of a chip (integrated circuit) that stores identifying data and antennas that collect energy and channels it to the chip to turn on. The tags' antennae are variable for the applications and can largely dictate how reliable the tags are.

RFID systems generally operate on one of three frequencies described in the table below. The frequency impacts the tag read speed, reliability (sensitivity to interference) and cost.

RFID Frequency	Band	Range	Tag Cost in U.S. dollars (approximate)	Considerations	Typical Use
Low Frequency (LF)	30 - 300 KHz	Short range, approximately 4 inches	$0.50 - 2.00	Slower read speed but low sensitivity to radio wave interference	Access control
High Frequency (HF)	3 - 30 KHz	4 inches - 3 feet	$0.50 - 2.00	Moderate sensitivity to interference	Ticketing, payment and data transfer
Ultra High Frequency (UHF)	300 KHz - 3 GHz (typical is 860 - 960 MHz band)	up to 40 feet	$0.07 - 0.15	Single global standard; Fastest read speed; Most subject to interference	Inventory management, anti-counterfeiting, wireless device configuration
Active RFID Tags (UHF)	300 KHz - 3 GHz (typical is 860 - 960 MHz band)	up to 325 feet	$25-100	Emit their own signal every 30 seconds	Large containers, railway cars, transportation systems

Source: rfidjournal.com, 2020

Readers

An RFID reader is the device that provides the connection between the tag data and the enterprise software that needs the information. The reader communicates with RFID tags within its field of operation, capturing data from them and passing it to a computer for processing. Like tags, there are many types of readers that impact their capabilities and cost.

Reader Type	How it works	Typical Uses	Approximate Cost in U.S. dollars
Handheld	Passive RFID handheld readers. A human being waves the scanner near assets	Manual auditing of a location, data center rack, etc.	$750 - 1,000 each
Fixed Position	Portal readers installed in a doorway that detect assets moving through	Event and ticketing (e.g. ski-lift passes, transport smart cards)	$500 and up per portal for hardware, installation and configuration
Active RFID Readers	Zonal readers that cover about 3,000 square feet detecting active RFID tags in their zone	Railway/cargo hubs, distribution warehouses	$500 - 2,000 each
Active RFID Rack/ Room Locators	Work in conjunction with Active RFID readers to report the precise rack or room location of the active RFID-tagged asset	Micro-location positioning: retail, amusement parks, etc.	$150 - 200 each

Source: rfidjournal.com, 2020

ACCESSIBILITY: MEDIUM (3)

What makes RFID systems so powerful also makes it one of the more difficult solutions from an accessibility standpoint. Deploying an RFID system requires multiple actors and many different components. Typically, installing a system involves basic hardware including tags, readers and reader control and application software. There are several great vendors out there but putting a program in place requires significant scoping and planning upfront as well as new infrastructure on both the sender (tag) and receiver (reader) side. (-2)

ACCURACY: VERY HIGH (5)

RFID accuracy varies by the type of tag, antenna and readers used, but it's possible to identify up to 1,000 tags per second at nearly 100% read rates. The main factors impacting accuracy are:

- **Frequency:** the higher the frequency, the more sensitivity to interference.
- **Tag antennas:** most tags have dual antennas to eliminate dead zones related to tag orientation. Some tags may also be optimized for the frequency band to improve performance.
- **Readers and reader antennas:** near-field systems have a shorter read-range and are less subject to interference. Far-field systems can read up to 100 feet, but have weaker communication.

Because of the maturity and range of options available with RFID, it's possible to make almost any use case work — for a price, of course.

SECURITY: HIGH (4)

Thanks to standard IP network security solutions, IP communication between RFID readers and the network is secure. The only real threat to RFID communication is between the tags and readers. Unlike beacons, which simply send a signal with a beacon identifier that effectively says, "I'm here!", RFID is transmitting data related to the product (the EPC or the Electronic Product Code). Data security threats are therefore present in the form of rogue/clone tags, unauthorized riders, and side-channel attacks (interception of reader data by an unauthorized device).

Some security measures have been built into all tags operating on ultra-high frequency (UHF) RFID, including disguised EPC number and kill commands that allow operators to deactivate tags so they don't send data. However, RFID has received some criticism for weak encryption, password protection and lack of tag or reader identification. (-1)

RFID security comes under scrutiny because, through the use of NFC applications (read more in the next chapter), it's increasingly become a go-to technology for payment and secure ticketing solutions.

COSTS: HIGH (2)

Because RFID solutions themselves are highly variable, so is the cost associated with them. While the cost has come down over time (corresponding to an increase in RFID use), high-volume transactions still make for the best business case.

For inventory unit level tracking, RFID is the cheapest automation solution out there. Passive tags can cost as little as $0.01 and some ultra-high frequency reader systems can process 1,000 tags per second.

The cost of an Active RFID tag is about on par with a beacon and they achieve similar battery efficiency and signal levels. Because Active RFID tags may operate on lower frequencies (~900 MHz) they may have a slightly lower risk of signal interference. However, the reader infrastructure for Active RFID is much more expensive. A single reader may cost up to $1,500 whereas an inexpensive smart device (as low as $50) may act as a reader in a BLE system. (-1)

Similarly, RFID systems for indoor navigation and location analytics are effective but the infrastructure can be extremely expensive. A 3,000 square foot space may have a signal zonal reader ($1,500) with several rack/room locators ($150-200 each) depending on the level of precision required. The same space can be fingerprinted using beacons for somewhere around $500-$850 and possibly less if it is already well-fitted for Wi-Fi solutions. (-1)

Finally, while RFID tags can be extremely cost-effective solutions for large volume objects, for people tracking, they still represent an incremental cost to the business where solutions like Wi-Fi and beacons are leveraging consumer-owned infrastructure (e.g. mobile phones). NFC systems (discussed in the next chapter) are a type of RFID, conveniently built into most devices and great for payment and ticketing applications. (-1)

VERDICT

RFID is best for anything that needs to be tracked at an item level or where some manual authentication is desired. RFID's ability to process thousands of items in seconds at high accuracy is unbeatable. Additionally, for applications where some human authentication (e.g. touch payments), is desirable, RFID is a great inexpensive option.

CHAPTER

05

NFC

Near-field communication (NFC) is most commonly known for its use in payments and transport ticketing (think about a subway card). As a form of passive RFID, it's energy efficient, creating its own power when in the presence of an NFC-enabled smart device. It can be used on one-way communication (tapping a smart card to a computer terminal for payment) or two-way communication (exchanging data between devices). However, per its name, NFC is a near-field communication system, meaning it only works within a four inch range. The table below represents some of the pros and cons of NFC systems.

Pros	Cons
Highly energy efficient and accurate Consumer controls timing and engagement with an NFC tag, generally preferable for secure transations Supported by Apple and Android Inexpensive, ranging from $0.10 - 0.60 per tag Works well with any contactless payment ternimal	Coverage radius is very small — 4 inches or less Consumer controls timing and engagement with an NFC tag — location analytics of room positioning require tags fixes to stationary objects and consumer-led transactions Not supported by Apple products prior to iPhone 6

Like all contactless data systems, NFC poses some major security concerns. To combat this, smartphone manufacturers have built additional security mechanisms into the chips that go beyond the security of traditional UHF RFID (for example, transmitting random one-time use codes in lieu of credit card numbers).

VERDICT

NFC is best for secure one-to-one transactions between a consumer and another entity (payment, transport ticketing). However, for security and cleaning contractors requiring location analytics, indoor navigation or proximity-based communication, it's likely that supplementary technologies would be required.

CHAPTER

06

GPS

Not only is the global positioning satellite (GPS) infrastructure completely universal, almost all modern smart devices are GPS receivers.

HOW IT WORKS

GPS is based on a constellation of 24 satellites circling the planet in one of six orbits. GPS satellites broadcast radio signals providing their locations, status and precise time. A GPS-enabled device receives the signal and uses its exact time of arrival to calculate the distance from each satellite in view. Once a GPS receiver knows its distance from at least four satellites, it uses geometry to determine its location on earth.

ACCESSIBILITY: HIGH (4)

Due to the ubiquity of both the transmitters and the receivers, GPS is a high accessibility performer. However, power use is still a downside for GPS technology. As anyone who has ever used Google Maps on a road trip knows, constantly searching for satellites is a huge battery drain and therefore a poor solution for always-on use. (-1)

ACCURACY: LOW (1)

GPS accuracy depends on several factors including atmospheric effects, sky blockage and receiver quality. Real-world data from the Federal Aviation Administration shows high-quality GPS receivers provide better than 12-foot horizontal accuracy. Higher accuracy is attainable using GPS in combination with augmentation systems. With these systems, accuracy is possible to within inches.

However, GPS accuracy breaks down indoors due to line of sight (e.g. no signal underground). Buildings block and refract the signal and multi-level buildings make it difficult to calculate altitude (which floor you're on). To use GPS for indoor location and positioning, it must be used in combination with nearby anchors or waypoints — most commonly, Wi-Fi. Since we're comparing technology as standalone systems and we're focused on indoor solutions, GPS receives a low score for accuracy. (-4)

PRIVACY & SECURITY: MEDIUM (3)

GPS is not invasive. It's simply four satellite signals recognized by a receiver and translated to location. The privacy and security risks are associated with the receivers (devices) and communication mechanism with the manufacturer's servers. A GPS receiver is as secure as the manufacturer has made it using authentication and storage techniques. However, given the variability of receivers and well-known hacker issues related to this, GPS receives a medium score on privacy and security. (-2)

COST: LOW (5)

While the infrastructure associated with GPS is an enormous cost, it's effectively free for the average consumer or business to tap into.

The main costs of GPS are the receivers — either personal devices or purpose-specific GPS trackers — and mobile applications required for business or use-specific purposes. Purpose-specific GPS trackers, particularly ones with security features built in and improved accuracy, can be very expensive. Also, augmentation systems to achieve better accuracy can be costly. (-1)

VERDICT

GPS continues to be the best location technology outdoors and especially over long distances. However, due to its battery appetite and lack of reliability indoors, GPS usually needs to be supplemented with other technologies for indoor location tracking.

CHAPTER

07

CONCLUSION

The right indoor location tracking solution depends on the goals of your business, existing infrastructure and constraints present.

WRAP-UP

Based on this research, BLE beacons have clear benefits that, at least for now, continue to have an important seat at the table. But that doesn't mean other technologies are null and void. The best solution for your business may be integrated solutions that consider the use case and environmental constraints to optimize the outcome.

Weighing the pros and cons of location technologies can be a massive endeavor. These systems are constantly evolving with new capabilities, features and price points coming out every day. This eBook attempted to represent facts and considerations for the average cleaning or security contractor, but you need to consult with other stakeholders to determine the best options for your business.

TEAM Software develops market-leading financial, operations and workforce management solutions for contractors with distributed workforces, with a focus on the cleaning and security industries in North America, Australia and the U.K. and Ireland. TEAM's fully integrated, holistic technology reduces risk and costs and drives efficiency, profitability and growth. More than 750,000 end users rely on TEAM's solutions globally. Founded in 1989, TEAM is headquartered in Omaha, Nebraska, U.S.A. For more information, visit teamsoftware.com.