

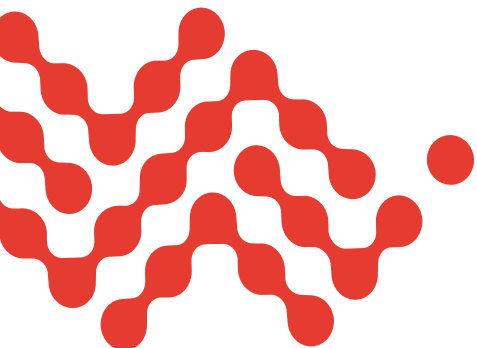


---

## How to Get IoT Connectivity Right

**Technological advances are creating a new wave of connected products that previously operated in isolation.**

This enables companies to control large numbers of products remotely, improving operational efficiency in the field. It allows them to constantly gather streaming information from sensors, creating opportunities for new services and reducing the cost of existing ones.



In this new world, everything from electrical infrastructure to public transportation is becoming data-enabled, creating new opportunities to make infrastructure more efficient. For many companies, previously unconnected products, from cars to wristwatches, are becoming delivery mechanisms for advanced services, and business models are rapidly evolving to capitalize on these new opportunities.

The Internet of Things (IoT) is enabling companies to digitalize their services, connect their products and improve their operational efficiency, but implementing IoT is very complex and has the potential to introduce new challenges:

- **Unclear ROI**  
Difficulties in assessing deployment and maintenance costs make it hard to predict economic benefits.
- **Complicated development**  
The cost and complexity of IoT developments can be difficult to predict and can escalate with unforeseen challenges.
- **Interoperability**  
IoT networks often involve thousands of devices that must work together, and engineering this can be complex.
- **Costly international deployment**  
Deploying IoT networks across different geographic regions means dealing with different connectivity service providers, which can be expensive and complex.
- **Ensuring security**  
Companies worry about the risk of data loss, but not all IoT deployments have robust end-to-end security.
- **Data privacy**  
If the data is sensitive and violates individuals' privacy, companies that suffer a breach could be subject to stiff penalties.
- **Unreliable service availability**  
Incomplete network coverage that may be acceptable for human users could lead to unsatisfactory service availability in IoT networks, because machines aren't always in the same place as humans.
- **Battery drainage**  
Devices must operate in the field for years at a time, making power considerations important.
- **Labor intensive maintenance**  
Sending maintenance staff out to repair hundreds to thousands of devices in remote locations is expensive.

### IoT Challenges

Support devices distributed over a wide area, including remote regions



Stay connected in challenging climates, or in moving vehicles



Devices must operate for long periods requiring low power usage



Building an IoT infrastructure can be time-consuming and complex

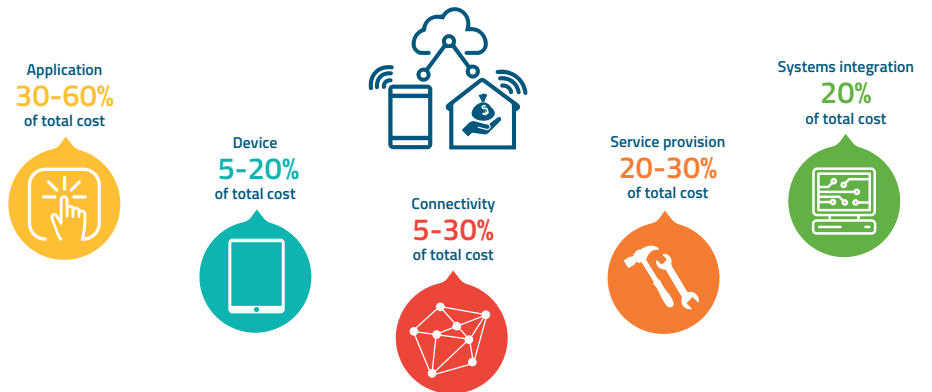


To overcome these challenges, companies need robust IoT connectivity, rugged devices, and intuitive applications.



Deployment teams can solve many of these challenges by building highly functional, reliable components at lower layers of the IoT technology stack. Connecting to wireless networks is a critical task for an IoT device. That connection can represent a significant cost in an IoT project, because it involves different service providers, connectivity plans, and technical challenges, such as maintaining the right bandwidth and reliability. To successfully connect your IoT application to the world, you'll need a solution designed to support these devices.

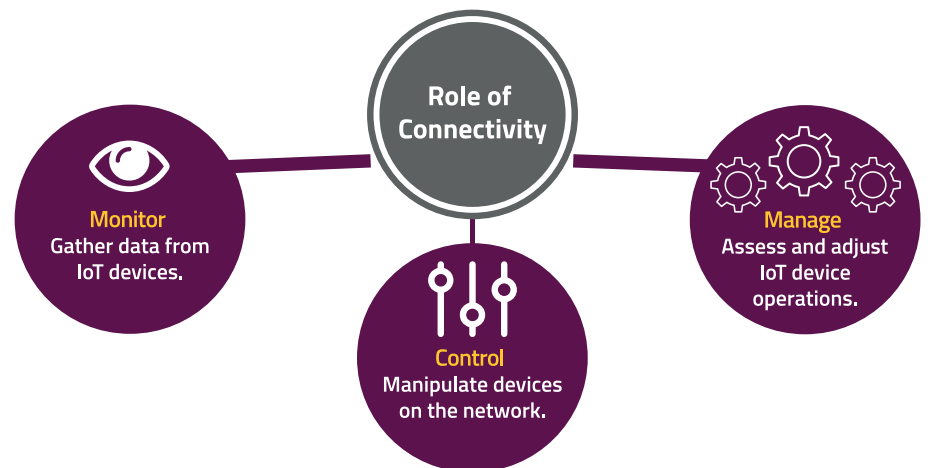
Yet for many companies, connectivity can be an afterthought in IoT implementations. They underestimate its importance and the cost of not choosing the right connectivity solution. This white paper looks at how businesses across different industries can get IoT connectivity right, putting them in a strong position to leverage the benefits that these transformative technologies can provide.



## The Key Role of Connectivity

Connectivity enables the best possible communication by creating a bridge between the physical and the digital world. It links physical devices, such as sensors and controllers, and the applications in the cloud that interact with them. A connectivity solution enables applications to interact with devices to monitor, control and manage them, as well as subscriptions.

An IoT-based service depends on the reliability and quality of the connectivity link. This makes connectivity an important building block in IoT infrastructure. Not only must it be reliable and offer the appropriate quality of service to serve the underlying devices and applications, but it must also be secure enough to stop sensitive data from falling into the wrong hands.



With the explosion of connected IoT devices, cellular operators are rapidly rolling out network solutions designed to support their unique needs. For example, Low-Power Wide-Area (LPWA) networks are being deployed globally to support devices with battery longevity considerations and low data usage, while plans for 5G high-speed networks are being rolled out for high-bandwidth devices. When it comes to deploying an IoT solution, companies should understand their connectivity needs before choosing a technology.

## The Benefits of Cellular Connectivity

There are several different technologies that can be used for IoT connectivity, but many suffer from significant drawbacks. It's important to understand your short and long-term needs and the strengths and weaknesses of the alternative connectivity technologies.

Wired networking is a non-starter for many IoT connections, for example. Economic considerations preclude hardwired connections to local area installations at short distances. These links make it time consuming, disruptive and expensive to move or add equipment. At first glance, local area wireless connections would seem to solve this problem. However, they can also suffer from management problems. Traditional Wi-Fi communications channels are subject to interference thanks to heavily overused 2.4 GHz bands. While 5 GHz is better, many Wi-Fi frequencies also use this spectrum today, and it is limited by shorter-distance coverage. These constraints make it more difficult to place and move IoT devices reliably. It's also a difficult technology to scale in large volumes, and its limited range makes it difficult to support collections of devices scattered across remote locations. Wi-Fi frequencies also have security risks; to learn more, read our white paper ["Risky Business: Avoid the Dangers of Wi-Fi with Cellular-Equipped Laptops."](#)

The most promising option is wireless wide-area technology. This enables large numbers of devices to connect over a broad area, giving planners the flexibility to change their infrastructure in line with business needs. However, network technologies based on unlicensed spectrum often carry risks. Quality of service is difficult to guarantee in unlicensed spectrum, which often limits downlink capacity due to regulatory constraints. This makes it difficult to manage and update devices in the field, which creates other quality and security issues.

As a result of these drawbacks, many companies are choosing existing cellular networks and standards rather than this unlicensed spectrum option. However, traditional cellular networks were not developed with IoT in mind. They were designed to support mobile phones, which have different technical requirements than IoT devices.

Many IoT devices must often operate for years in the field, calling for extremely high energy efficiency and low power usage. This gives IoT devices more power constraints than the smartphones that cellular networks were designed to support.

Reliability is another factor. Many IoT devices operate independently and may simply stop working if the connection fails. They must also operate in challenging environments, including deep indoors or underground, in moving vehicles and in extreme environmental conditions. These factors make it challenging to use conventional SIMs, creating lapses in coverage and interruptions in transmission. Using traditional SIMs for IoT applications increases complexity and is not the most effective long-term solution for connecting billions of IoT devices.

To tailor wide-area wireless communications for the IoT era, standards bodies and vendors have developed 4G Low-Power Wide-Area (4G LPWA) network standards. These offer appropriate technical properties for IoT use cases, covering wide areas and prioritizing energy efficiency. There are two types of LPWA technology standards developed by 3GPP.

- **Narrowband IoT (NB-IoT)**

Also known as Cat-NB1 offers average rate bandwidths of between 20-65kbps, although these can reach peak rates of up to 250Kbit/sec. However, there are limitations of NB-IoT (including no inbound roaming and no voice or SMS support).

- **LTE-M**

Also known as LTE Cat-M1, it is a fast, low-power system offering up to 375kbps at very low latencies, making it suitable for every IoT use case including smart metering as well as those requiring voice capabilities, mobility and roaming, such as health monitoring, fleet management and home security.

LPWA protocols, based on existing cellular standards in licensed spectrum, offer several advantages. One lies in consensus and control. As internationally agreed, standards with many stakeholders, these technologies have a clear and reliable governance process that protects stakeholders' interests. They are also designed for extremely low-power consumption and provide better connectivity than shorter-range protocols.

The other benefit lies in interoperability. Whereas proprietary technologies can include opaque elements in their technology stacks, the interoperability of 4G-based LPWA technologies are tried and tested by many large, powerful stakeholders. Equipment is easy to make interoperable, minimizing the risk for everyone in the value chain. 4G LPWA protocols have now been rolled out extensively around the world.

Selecting one of the cellular 3GPP standards for LPWA will ensure global coverage, industry interoperability and a path to 5G, which is important as older networks begin to be phased out.

## Benefits of Cellular Networks for IoT

<b>Ubiquitous</b>	Coverage across almost the entire world means that companies can connect their IoT device from virtually anywhere.
<b>Standardized</b>	Based on the well understood and globally deployed 3GPP standard.
<b>Secure and reliable</b>	Mobile network operators (MNOs) have made huge investments in their networks to assure signal quality, security and availability and are contractually obligated to deliver Quality of Service (QoS).
<b>Cost-effective</b>	MNOs are responsible for deploying, operating and managing wireless communications, which is both simpler and lower cost for companies.
<b>Mission-critical data</b>	Cellular can be used for any type of data transmission – from basic location or temperature data to images and video – and uses data encryption by default, giving companies better security.

## 6 Considerations for IoT Connectivity

For companies looking to implement an IoT solution, there are six crucial considerations:

- **Coverage**

In many IoT deployments, infrastructure will have to span many different geographies, each with different carrier coverage. Managing multiple SIM vendors across a global deployment is challenging. Infrastructure will also have different coverage requirements based on the use case. An urban deployment may require support for dense clusters of devices to serve a tightly packed population, for example, whereas a rural implementation may serve a sparse population spread across a wide area. Design teams also need to consider the extent to which the IoT network must provide indoor coverage. Extending communication inside buildings introduces a range of technical issues, such as frequency considerations and density of device placement. Or your deployment may only require regional coverage, for example just in the US or Europe.

- **Data quality**

Many IoT deployments support mission critical business processes or are in sectors that are part of the critical national infrastructure. Their connectivity solutions must preserve data integrity and reliability, delivering data streams consistently so that networked IoT devices can support accurate, timely results for applications running mission critical processes. However, companies can face frequent connectivity issues, with local gaps in coverage or prolonged outages, especially if they have a single network provider.

- **Scalability**

A collection of connected IoT devices will also provide the basis for managing potentially millions of devices spread across a wide area. An IoT connectivity solution must therefore be able to scale. Monitoring the state of IoT devices across the network and controlling their operation relies on a robust connectivity layer.

- **Easy to build**

With potentially millions of devices to support, connectivity solutions must be simple to configure and set up. Connecting machines and assets can be hard, especially on networks designed primarily for consumer devices.

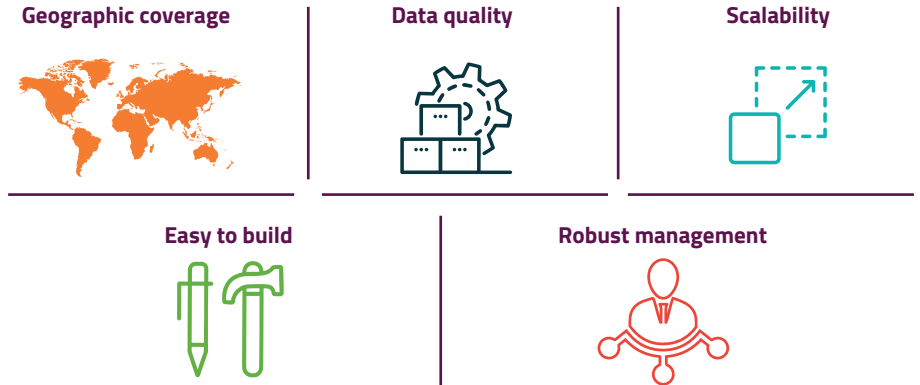
- **Robust management**

Companies may have to manage millions of devices spread across a wide area. Monitoring the state of IoT devices across the network and controlling their operation requires a robust connectivity and management layer. They have to be able to monitor and maintain secure device connections. Network disruption or local coverage gaps may cause devices to go offline for periods. At the same time, when a network fails it can often be inundated with calls, causing slow response times.

- **Flexibility**

Many pricing plans are inflexible and do not suit the operational needs of companies. For example, one firm may have major seasonal spikes in activity and need plans that reflect this. Also, with large distributed networks it can be hard for companies to track their data expenditure in real-time, making it easy for them to over-spend.

There are a broad range of IoT connectivity options. The challenge is to select the best connectivity solution for your IoT deployment.



**IF YOUR PRIORITY IS TO ENSURE RESILIENT GLOBAL CONNECTIVITY FOR IOT DEPLOYMENTS**

Traditionally, cellular network providers have used their own SIM cards to authenticate and communicate with devices on their network. This approach was not designed with IoT devices in mind and carries several drawbacks.

First, network-operator-owned SIM cards increase complexity when an IoT deployment targets different geographies. Companies that want to position connected devices in multiple countries and even multiple regions will need to deal with different cellular network providers and different implementations of connectivity protocols. This is difficult, and time consuming for IoT deployment teams to manage and provides little flexibility as deployment locations or business needs change.

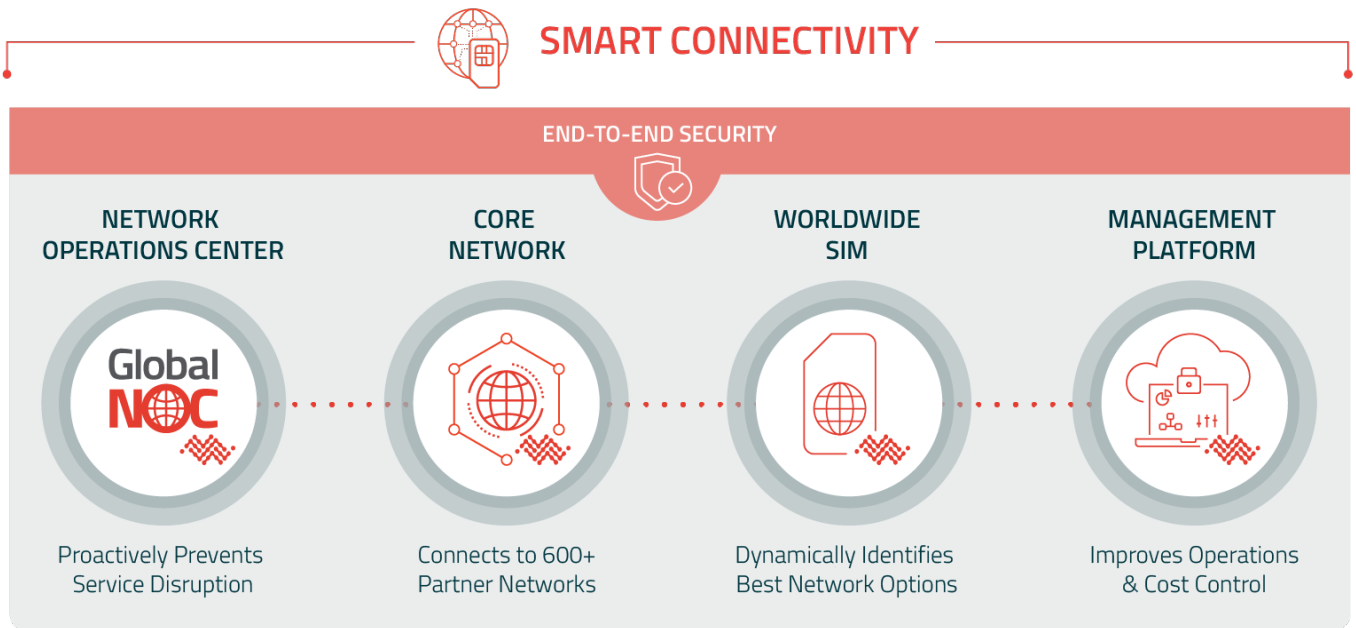
Using traditional SIMs for IoT connectivity can also carry performance and reliability implications. Reliance on a single network provider can cause lapses in data transmission when a network suffers an outage or its coverage is not optimal for a device’s location. This creates a single point of failure and can leave IoT deployment teams relying on a single provider for support, which can be problematic in a mission critical environment. Also, a single provider may have an incomplete coverage map, which can be problematic for devices located in rural areas or operating deep indoors.

With so many different geographies to manage, and with so many different providers and commercial policies, companies deploying IoT solutions might feel overwhelmed. This makes the ability to manage devices from a single source highly appealing for deployment and management teams that want a simple, scalable and dependable solution. Sierra Wireless' Smart Connectivity solution provides a single worldwide SIM that connects to over 600 partner networks in over 190 countries. This makes it much easier to manage logistics for global deployments. Whichever country or region a company is operating in, Sierra's patented technology devices are automatically connected to the optimum network available. By constantly scanning for and connecting with the highest-quality networks in a given location in real-time, it also maximizes data quality across all these geographies.

Smart Connectivity technology supports the GSMA's Remote Provisioning Architecture for the latest Embedded UICC eSIM technology standard, which enables companies to remotely change the connectivity provider on the worldwide SIM at any time.

Smart Connectivity also provides resilient global coverage. Sierra Wireless' core network delivers secure redundant routes to multiple networks in each country thereby eliminating local coverage gaps.

In addition, Sierra Wireless' Global Network Operation Center (GNOC) runs 24 hours a day, 365 days a year. We are constantly monitoring our core network throughout the world and working proactively to prevent service disruptions. If there is an outage, we have direct communication lines with network operators, so we can troubleshoot the issue.



## IF YOUR PRIORITY IS TO SIMPLIFY IOT DEPLOYMENTS AND REDUCE TIME TO MARKET

Sierra Wireless's Ready-to-Connect solution removes the main barriers to a successful IoT deployment. It offers modules and routers embedded with pre-integrated global connectivity, IoT operations management and security. This simplifies the deployment of IoT devices in several ways:

- **Simpler development**

Ready-To-Connect solution decreases time-to-revenue by eliminating several time-consuming development steps in the development of an IoT solution. It offers e-SIMs inside of its modules, gateways and routers that provide instant access to Smart Connectivity and eliminates the need to provision devices individually. The solution takes care of front-end connectivity hardware development, the protocols and standards work, device and connectivity management, security and user administration.

- **Centralized connectivity and device management**

Sierra Wireless' IoT platform manages all SIMs, subscriptions and devices out of the box, through a single interface. All new devices and SIMs are paired and pre-declared into the platform when shipped, which highly simplifies integration. With such a degree of integration from the device to the cloud, Ready-To-Connect guarantees a low start-up time and a high level of security. Sierra Wireless' embedded modules provide instant connectivity to more than 190 countries at power-up. There is no need to integrate them into the management platforms of other vendors, which can be costly and time consuming. You can also activate, change or suspend subscriptions with no restrictions, anytime you like, over-the-air.

- **Streamlined operations**

Ready-To-Connect enables customers to deal with a single supplier when building the connectivity layer of their IoT solution. It eliminates the need to deal with multiple SIM procurement partners, and Sierra Wireless' e-SIM technology makes it easier to switch cellular providers remotely when necessary.

- **Integrated pricing**

Instead of negotiating multiple prices and different contracts with network operators, the Ready-to-Connect devices provide instant access to Smart Connectivity, which includes all the necessary network subscriptions pre-managed, with a pricing model customized to suit IoT infrastructure needs.

- **Strengthen end-to-end security**

Concealed e-SIMs help prevent SIM tampering or theft. Meanwhile, Sierra Wireless use the latest encryption technologies in the device, network, and cloud, providing further protection.

- **Reduce management resources**

Together, these capabilities enable organizations to lower the cost of managing their IoT deployment by reducing the complexity of management, upgrading firmware easily and increasing visibility. It also helps reduce the cost of managing commercial provider contracts, which can otherwise quickly escalate and become expensive.

Ready-to-Connect devices provide a one-stop, streamlined answer to the following questions:

- How do I communicate with my devices?
- What protocol do I use to transfer data?
- How do I diagnose field issues?
- How do I keep connectivity costs under control?
- How do I secure it all?
- How do I make sure my staff can access the solution and manage everything as simply and cost effectively as possible?

### IF YOUR DEPLOYMENT IS SOLELY IN NORTH AMERICA

Some companies do not necessarily require all of the global capabilities of Smart Connectivity. For example, if a company is solely operating in North America, it can opt for Sierra Wireless' Enhanced Carrier Connectivity, which helps to simplify and optimize deployments in that region. This integrated service provides a single source for selecting and managing multiple Tier-1 carriers in North America. Clients can then optimize their deployments based on the best coverage available in any given area.

The service provides great flexibility and transparency as users can receive monthly data pooling for each carrier and can suspend plans at any time. In addition, they can more closely manage costs, as there are automated usage alerts. If budgets are breached, then devices can be automatically suspended.

As with Smart Connectivity, Enhanced Carrier Connectivity is also supported by Sierra Wireless' GNOC that constantly monitors our core network to make sure there are no services disruptions. It is closely integrated with Tier-1 operators in North America to help us prevent downtime and avoid any local coverage gaps.

## Single Point of Management

No matter what a company's connectivity needs may be, Sierra Wireless provides all the options necessary to support any IoT deployment. Whether it's Smart Connectivity or Enhanced Carrier Connectivity, Sierra Wireless provides a single point of management and accountability. This reduces the amount of time it takes to identify the root cause of any outages and solve any problems. Sierra has over 25 years of devices and network and device troubleshooting experience. Meanwhile, our single device and cloud management platform provides a unified view across all your carrier SIMs, whether they are from Sierra Wireless or another service provider. This improves operational efficiency and helps companies monitor costs. Every point in the connectivity lifecycle is enabled in our IoT platform, including SIM ordering, activations/deactivations, monitoring, activity alerting and billing, as well as additional IoT functions, such as device management. In addition, every feature and service in the web portal is fully available via APIs for easy integration.

## Conclusion

Modern technology development demands fluid, adaptable infrastructures that are both functional and resilient. As companies build out their IoT solutions, they have a once-in-a-decade opportunity to create a connectivity layer that will support their future needs. But all IoT deployments involve technical challenges. Partnering with a single company, with real expertise in the field, that can lead or coordinate development, is often the most effective way for businesses to move forward, as it reduces complexity and makes every step of the set up easier to manage. An experienced partner can leverage its core technical strengths and help a company reach new levels of innovation both now and in the future.

The business world is evolving at a breakneck pace, driven by rapid technology innovation. Tomorrow's business will be substantially different than today's, and those companies will call upon connected IoT devices in new and exciting ways. The investments that IoT adopters make now must support future developments.

By designing IoT ecosystems with the future in mind, companies can protect their investment and position themselves to be agile and responsive. This means designing hardware and connectivity systems to be flexible and easy to scale up as needed. Having a future-proof connectivity layer that can be adapted and reshaped to suit emerging requirements is not just a welcome option – it's a requirement. Redeveloping an entirely new connectivity layer in the future will not be an option for most IoT deployments. Companies must get it right the first time.

Start with Sierra, your trusted partner for IoT success. We are a leader and innovator in the IoT, with more than 25 years of networked device expertise. Our core strength is our ability to provide an end-to-end solution that supports a company from concept to deployment to operation.

## THE SIERRA WIRELESS DIFFERENCE



### Simplify Global Deployments

One SIM for deployments anywhere in the world and the widest range of ready-to-connect devices



### Maximize Coverage

Best available network selection with redundant routes to multiple networks in every country



### End-to-End Security

Tightly integrated device-to-cloud solutions with deep industry and security expertise



### One Point of Accountability

One partner to call for support with 25 years experience in device and network troubleshooting

### About Sierra Wireless

Sierra Wireless (NASDAQ: SWIR) (TSX: SW) is the leading IoT solutions provider that combines devices, network and software to unlock value in the connected economy. Companies globally are adopting IoT to improve operational efficiency, create better customer experiences, improve their business models and create new revenue streams. Whether it's a solution to help a business securely connect edge devices to the cloud, or a software/API solution to help manage processes associated with billions of connected assets, or a platform to extract real-time data to make the best business decisions, Sierra Wireless will work with you to create the right industry-specific solution for your next IoT endeavor. Sierra Wireless has more than 1,300 employees globally and operates R&D centers in North America, Europe and Asia.

For more information, visit [www.sierrawireless.com](http://www.sierrawireless.com).

Connect with Sierra Wireless on the IoT Blog at [www.sierrawireless.com/iot-blog](http://www.sierrawireless.com/iot-blog), on Twitter at [@SierraWireless](https://twitter.com/SierraWireless), on LinkedIn at [www.linkedin.com/company/sierra-wireless](http://www.linkedin.com/company/sierra-wireless) and on YouTube at [www.youtube.com/SierraWireless](http://www.youtube.com/SierraWireless)