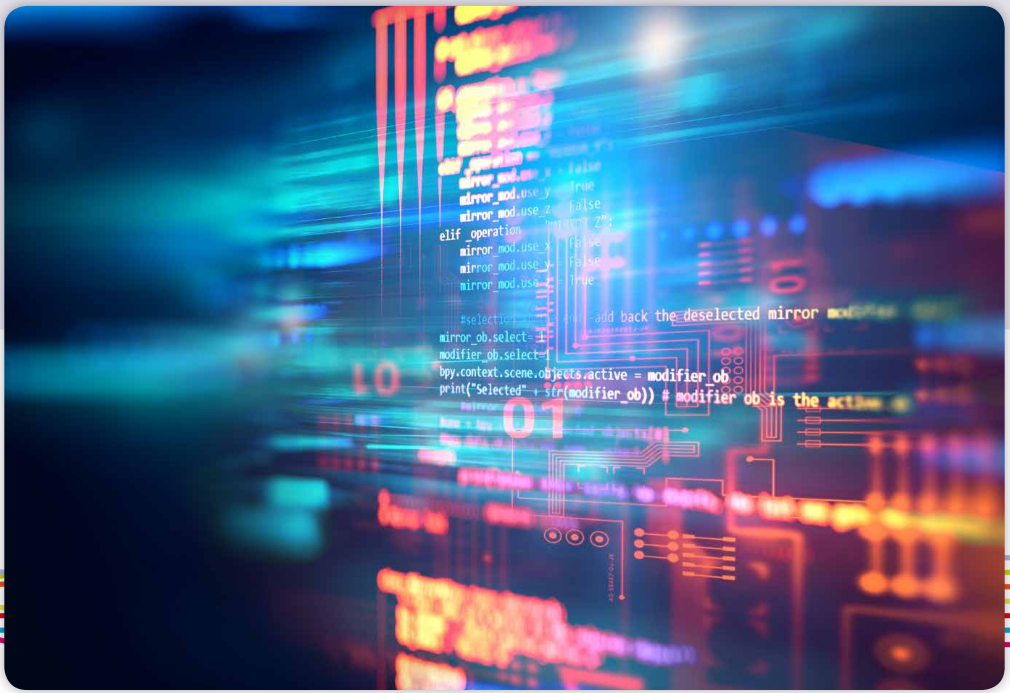
Business-Critical IoT Connectivity Solutions: **Key Management Challenges**



Sponsored by:

SIERRA WIRELESS®

beecham research

Shaping the IoT future

The growing need for 'always on' connectivity

The IoT (Internet of Things) is all about connecting remote devices and then gaining useful data from them for processing and use in applications. The connection itself is crucial – no connection, no data. As that data becomes more critical to operations, then so does the connection delivering it.

With many more 'things' being connected as part of the IoT, one of the big challenges that enterprises are facing is ensuring 'always on' connectivity for their devices wherever they are and however many they have. There could be many thousands. This is particularly the case for service providers and device OEMs, who may have global operations, where being connected is closely related to the service they offer – no connectivity, no service. That service may increasingly in future be a managed service where the cost of the device itself is included in the service charge as part of a Device as a Service (DaaS) business model. How do they find the best connectivity for their devices, providing the coverage and the data speeds they need? More to the point, how do they manage that connectivity?

In addition to the connectivity itself there are other challenges as well, for example when expanding in multiple regions there is a high need for control and security – ensuring these are also effectively managed. Yet if you do not have the connectivity, you cannot reach the device. So, in the end it is really the global IoT connectivity that is the key and, in addition to that, there is a need to ensure the best coverage in each region.

Traditional SIM cards add to the challenges

The traditional SIM card (Subscriber Identity Module) has contributed significantly to the growing success of the mobile handset market for many reasons. This has included its easy access and wide availability, extensive network coverage and inherently high network security. It has also catered for the ability to select and change the mobile operator the user wants at the point of sale in a retail outlet.

But it is not ideal for other connected devices which are not purchased through mobile phone shops. This is the case for the vast majority of IoT applications. For these, matching up the SIM card and device occurs at a different point in the supply chain, which can be difficult and time-consuming. It introduces new and sometimes costly logistical issues. In addition, if there is a need to change the mobile operator during the life of the application for whatever reason, it means changing the SIM card – which is locked to one carrier – and that introduces other logistical issues. It may, for example, require a site visit. Even when on site, the card may be physically difficult to access. It may require a ladder to reach it. It may be in a locked cabinet out of easy reach. On the other hand, if it is easy to access and in a public location, it may then be open to tampering and even theft. Such issues and more all add cost and further logistical challenges in the use of SIM cards for connected devices.

This is why the eSIM (embedded SIM) solution has been introduced. It enables provisioning over the air, which makes it possible for the network operator connected to the SIM to be assigned or changed remotely. The major advantage for OEMs of this approach is that the SIM can be inserted into a device's circuit board during manufacture like any other component and then provisioned later with the appropriate network operator profile for wherever in the world it happens to be. It converts the SIM into a single SKU (Stock Keeping Unit), thereby helping to streamline production processes and reduce costs. This is particularly important for the OEM market where products may be shipped anywhere in the world.

The eSIM solution dramatically opens up the opportunities for OEMs to use cellular connectivity in their products. It has already been taken up by the auto industry manufacturers, who have pioneered its use, and is relevant for any application where embedded, wide area connectivity is appropriate. Through the way it works, this solution also changes the ownership of the SIM itself. The traditional SIM card has always been the property of an individual network operator. It is supplied by the operator and to change operators requires a physical change of SIM. With the eSIM solution, the SIM in the device is owned by the OEM or service provider. It is then up to them to decide which network operator is most appropriate to connect to, wherever the device is located. These are all issues that need managing.

Adding value through IoT connectivity

The more services and data that are delivered through an IoT connection, the greater the value of that connection and the more important it is that the connection is effectively managed.

Figure 1. *Increasing Value of an IoT Connection – Towards Mission Critical*

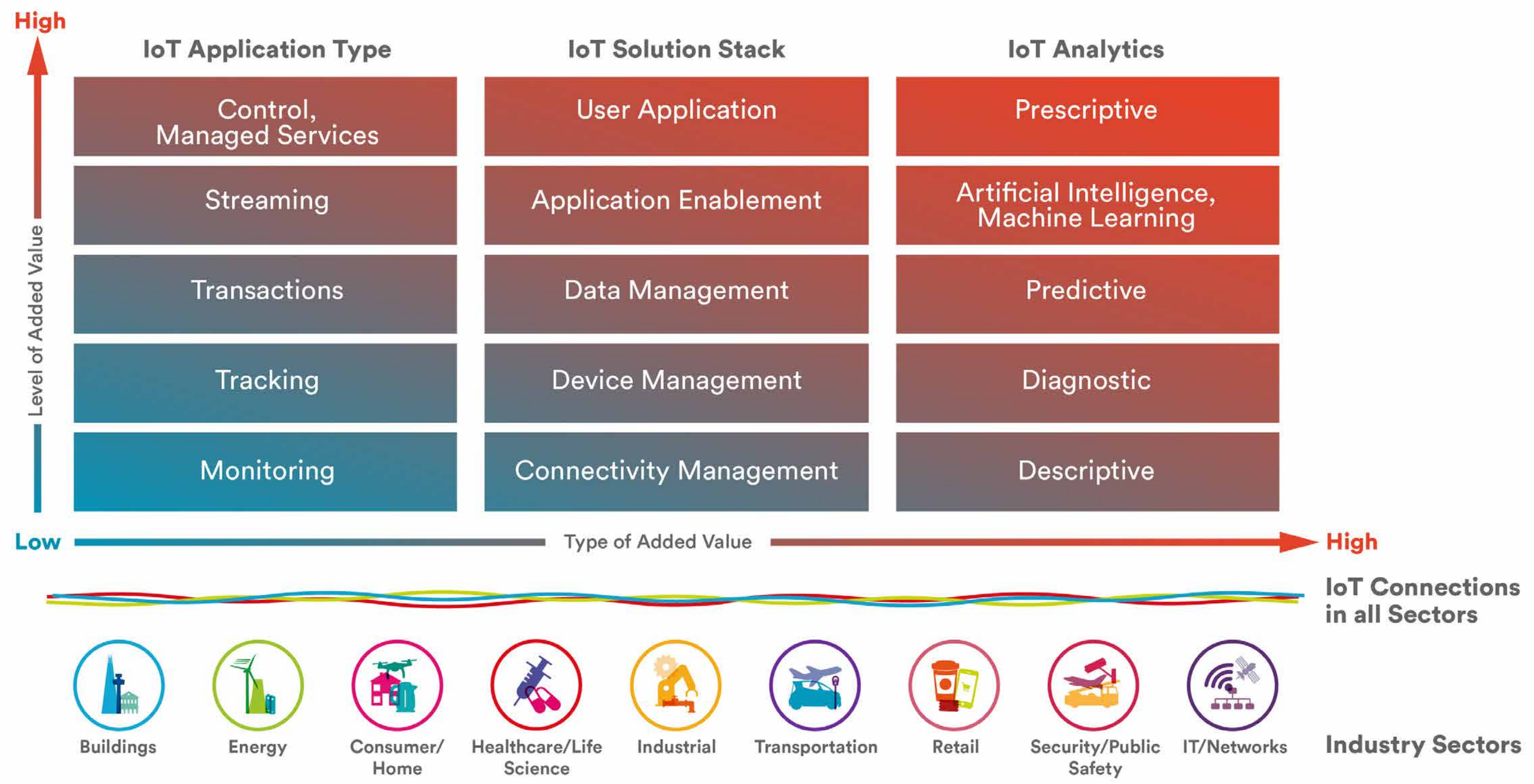


Figure 1 illustrates the increasing value of an IoT connection over time: once a connection is installed, there is a route for adding new value to the business operations. It applies to the connection of devices for applications in any of the 9 identified industrial sectors. Typically, it is first established for a simple operation, for example a simple monitoring activity as shown in the bottom left. That may then evolve through the other levels of the IoT Application Type stack, towards a higher value, remote-control activity or even a fully managed service where the value of the device itself can be paid for as a service – the DaaS model discussed on page 2.

As the application becomes more important to the business operations, it is increasingly important to manage all aspects of the connectivity (Connectivity Management) to ensure the application is not disrupted by the connection being broken, not working correctly or being hacked. The eSIM solution, although closely associated with Connectivity Management, is yet another quite separate process that relies on the connection itself being maintained. At the same time, it also becomes more important to manage the connected device itself (Device Management), for example, to ensure it has the latest firmware. The data coming from the device needs to be managed as well (Data Management) and new applications need to be developed and then made available to the user (Application Enablement and User Application). All of those increasingly valuable activities rely on the IoT connection being maintained. If the connection goes down, all of them are lost.

Then we come to the use of that data. Figure 1 shows this as an IoT Analytics stack. Essentially, each higher level of this stack requires more data. At the same time, each level adds more value to the overall service or solution being offered, and the connection itself becomes even more critical. As the data coming from the connected device becomes more important to operations, it becomes necessary to process it in new ways to add further value. This involves taking IoT Analytics from simple Descriptive and Diagnostic activities through to Predictive activities, such as preventive maintenance. Adding an Artificial Intelligence and Machine Learning level makes is possible to reach a Prescriptive level, where actions can be taken to optimise performance.

Overall, it means there are several added value stacks that are enabled by the IoT connection, moving both up the chart and across it from left to right. At each stage, the underlying connection itself becomes more important to operations – becoming mission critical. This is why it is so important when choosing the most appropriate connection for a remote device that future needs are considered at the beginning – as part of the plan. It is also why everything surrounding that connection must be managed effectively and in a coordinated way.

Managing the IoT Connectivity Challenges

Specifically, what must be managed effectively for an IoT connection to perform as required? Unlike mobile handsets, IoT devices are often deployed in large fleets or populations that must be kept online at all times and need to be actively managed remotely. For business use, the network must be available with sufficient coverage wherever it is needed. Also, the quality of network service available must be sufficiently high to ensure the services offered, or data collected, can operate effectively. In addition, the devices themselves must be able to operate for a sufficiently long period in the field. Looking at these issues in more detail:

The network must be available with sufficient coverage wherever it is needed.
In the consumer space, mobile phones spend most of their time in a particular region and travel outside that region infrequently. Roaming is the exception, not the norm. Traditional SIMs and networks have been designed to minimize these roaming costs, usually at the expense of performance and reliability.

For IoT devices working with traditional SIMs, the charges associated with roaming can be crippling. An IoT device can be deployed in any geographical region, far away from the factory or the corporate headquarters that represents “home.” The IoT devices used in automotive and transport applications are in near-constant motion, passing through any number of cellular coverage areas on a regular basis. Even IoT devices that are fixed in place, and never change their location, are still roaming, from a cellular point of view, since they have been commissioned for use somewhere other than “home.” In the IoT, roaming is a constant.

The quality of network service available must be sufficiently high to ensure the services offered, or data collected, can operate effectively.
Today’s smartphones may make extensive use of data, but voice calls remain an important part of every cell-phone’s functionality. People still equate good cellular performance with fewer dropped calls, and if they find themselves in an area where data connectivity is not very good, it is not critical – they just try again later, when they are in a different location with a better connection. For IoT devices, however, data connectivity is critical. What is more, IoT devices operate independently, without human intervention. If an IoT device finds itself with a voice-only connection, it may be stuck, since there is no one there to re-establish the connection. The device may be saddled with a useless connection and, unable to send data for an extended period. Most businesses cannot afford to operate with IoT devices that go dark and cannot transmit, nor can the business models support service calls to fix connectivity issues in remote locations. So, it is essential that IoT devices can consistently find and keep a high-quality connection

The devices themselves must be able to operate for a sufficiently long period in the field.
The average mobile phone has a lifespan of about two to three years. Cell-phone users can easily swap out the SIM, in a process that takes just seconds, and whenever they buy a new phone, they are also getting the latest SIM technology. The average IoT device might stay in the field for more than a decade, in a hard-to-reach location, with an embedded SIM that is difficult to access. Swapping out SIMs, to support a different provider or upgrade to a newer generation of cellular, can mean an expensive field-service call, and may require special tools and the expertise of a trained technician. Also, having to stock different SIMs, for use in different geographical locations, can increase the cost of operations and make it harder to manage inventories.

Managing the IoT Connectivity Challenges: User Survey

To find out more about what business users think they need to address these challenges, Beecham Research recently conducted a large IoT connectivity survey among enterprise users and product manufacturers. This specifically focused on their use of cellular for IoT, the challenges they face and their expectations for eSIM (embedded SIM).

Figure 2 key findings from this were:

Managing multiple vendors – 69% of respondents considered this to be quite or very challenging.

Reducing TOC and BPM cost – 78% considered this to be quite or very challenging.

Scaling globally – 80% considered this to be quite or very challenging.

Reducing time to market – 66% considered this to be quite or very challenging.

These are very high numbers and represent significant findings.

In **Figure 3** we then asked about their preference in managing these elements, whether they prefer a single partner to be responsible for all, or potentially different partners for each element. Their response showed a clear preference for one partner at 56%, although the different partners option at 44% also scored quite highly, so we investigated this further.

Figure 2. *To what extent do you view these as challenges for your IoT Connectivity?*

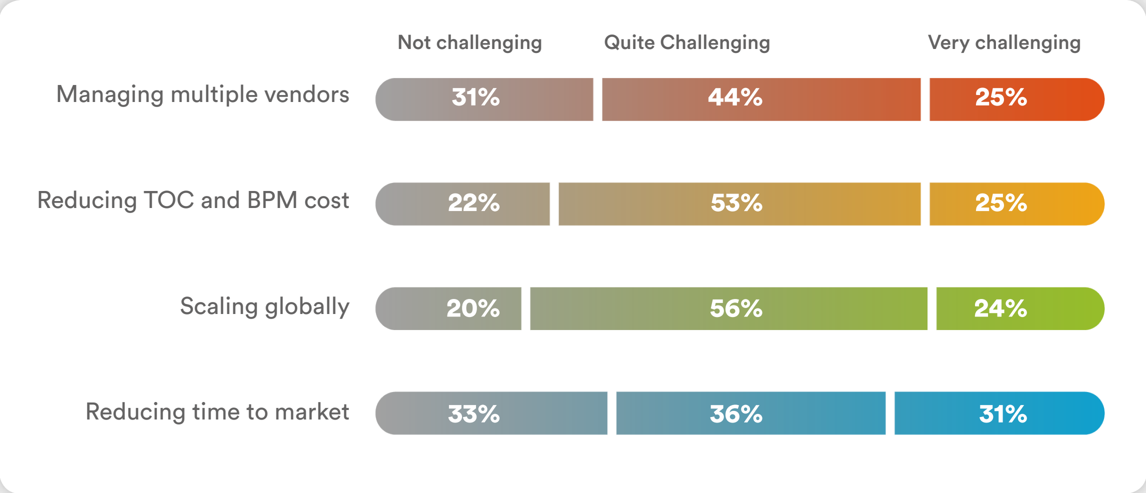
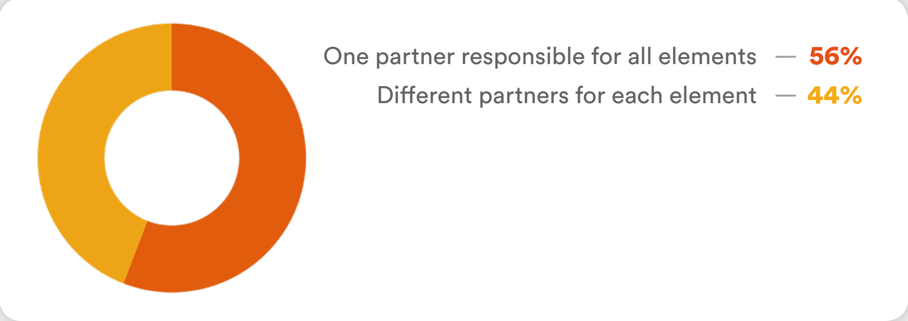


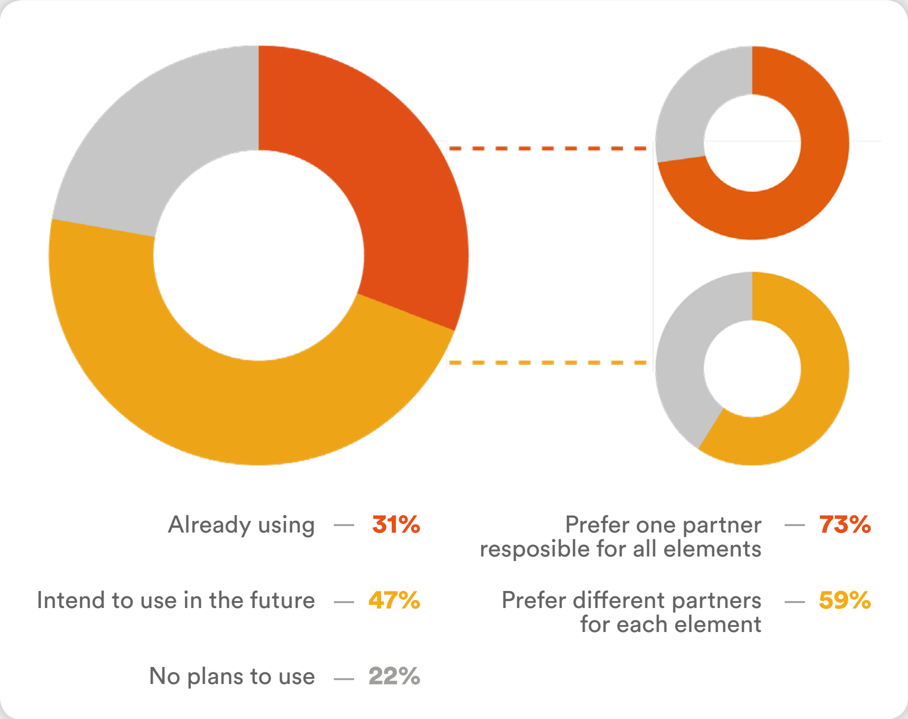
Figure 3. *Managing these elements, would you prefer to work with:*



In **Figure 4** we asked about existing or expected future use of eSIM. A very large majority of 78% were either using or expected to use eSIM in the future. This confirms the very high interest in use of eSIM for IoT over the next few years that we have seen elsewhere in the market.

A particularly striking finding then came by cross-referencing responses to the questions in Figures 3 and 4. This showed that, among those already using eSIM, the answer to the question in Figure 3 was in fact 73% in favour of a single partner, whereas for those intending to use eSIM in the future the answer to the question in Figure 3 was 59% in favour of different partners. This indicates a strong difference of opinion among those currently using and those intending to use eSIM. We would suggest that those currently using eSIM are more aware of the issues involved in managing eSIM and may well have changed their minds in light of this experience.

Figure 4. *To what extent do you use or intend to use eSIM?*



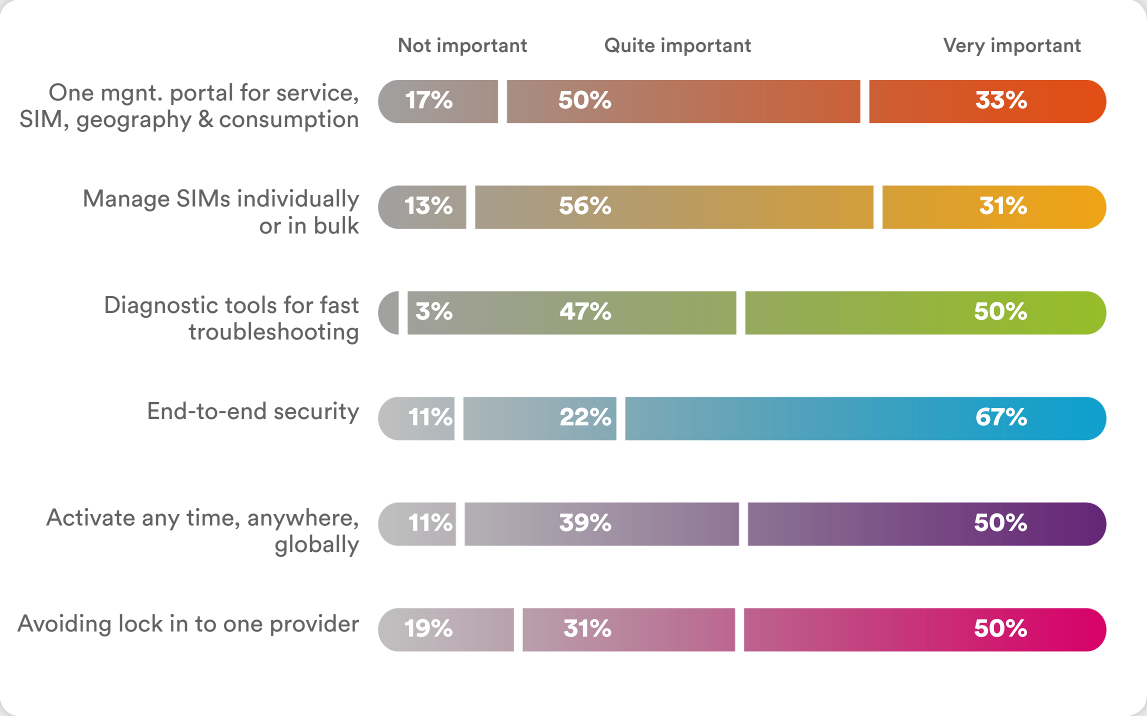
As shown in **Figure 5**, we then asked which eSIM attributes they considered to be most important for their businesses. This covered a wide range:

1. One management portal for service, SIM, geography and consumption
2. Manage SIMs individually or in bulk
3. Diagnostic tools for fast troubleshooting
4. End-to-end security
5. Activate anytime, anywhere, globally
6. Avoiding lock in to one provider.

Item 6 on this list refers to one carrier as provider – being locked in to one carrier, either directly or directly through a reseller.

Not unexpectedly, item 4 (end-to-end security) has the highest score for Very Important (67%). This attribute consistently scores highest in similar surveys. However, when combining Quite Important and Very Important scores, item 3 (Diagnostic tools for fast troubleshooting) comes out top by a wide margin at 97%. This indicates the high interest in using diagnostic tools together with eSIM to quickly identify and deal with issues arising in the field – where physical visits are often not practical. Again, when combining those two scores, each of the attributes scored over 80% (the range being from 81% to 97%). This emphasises the perceived importance of all of the attributes when managing an eSIM portfolio.

Figure 5. *Which of these eSIM attributes is important to your business?*



These findings closely reflect the management challenges noted earlier:

- The network must be available with sufficient coverage wherever needed. ‘Activate any time, anywhere, globally’ was consider quite important or very important by 89% of the survey sample.
- The quality of network service available must be sufficiently high to ensure the services offered, or data collected, can operate effectively. ‘One management portal for service, SIM, geography and consumption’ was considered quite important or very important by 83% of the survey sample. In addition, ‘Managing SIMs individually or in bulk’ also has a bearing on this issue and was considered quite important or very important by 87% of the survey sample
- The devices themselves must be able to operate for a sufficiently long period in the field. ‘Diagnostic tools for fast troubleshooting’ was considered quite important or very important by a stunning 97% of the survey sample.

Sierra Wireless Smart Connectivity service

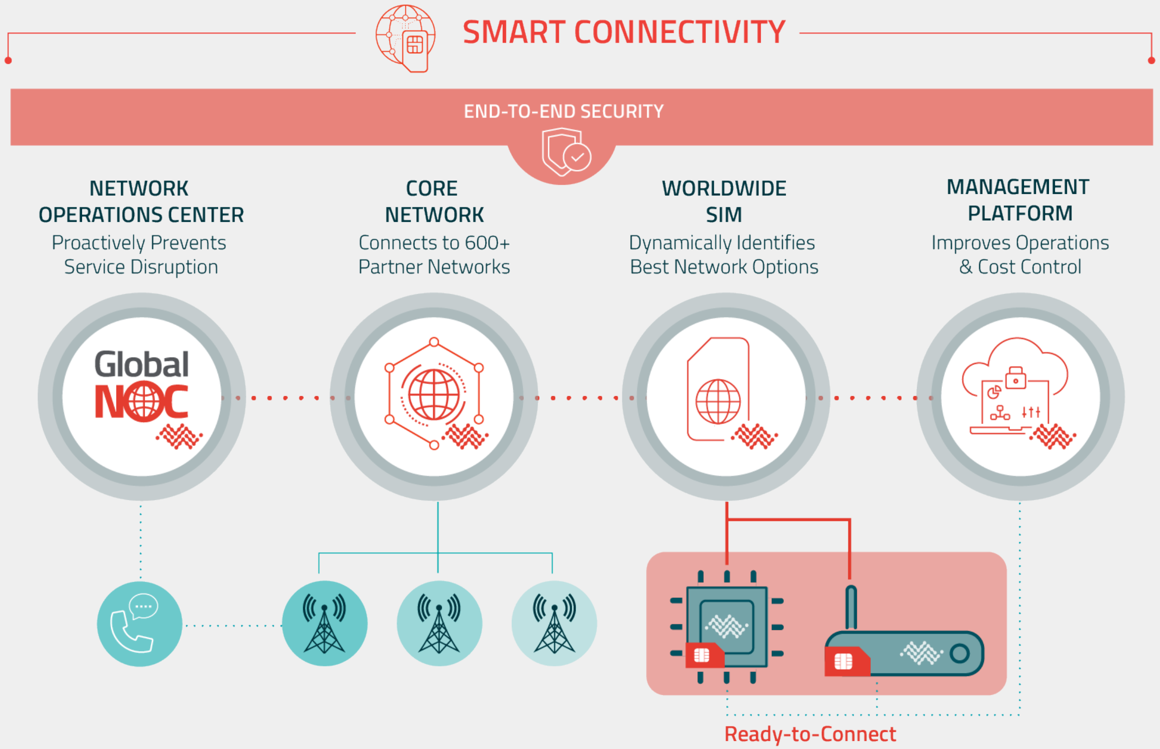
Sierra Wireless has addressed each of these management issues with its Smart Connectivity service, which is designed to simplify and augment global IoT deployments. This service makes it easy to maintain a secure and reliable connection to both fixed and mobile assets anywhere in the world. It also provides multiple redundant routes to 600+ partner networks in order to eliminate local coverage gaps. Instant access to the service is enabled by Ready-to-Connect modules, gateways and routers. eSIMs that are pre-integrated inside Ready-to-Connect devices can be activated over-the-air, thereby eliminating individual device provisioning. If there is an outage, the eSIM automatically selects the next strongest, available network in the area.

As shown in **Figure 6**, Smart Connectivity provides secure and resilient global coverage and includes the following key components:

- Network operations center – Proactively prevents service disruption with 24/7/365 monitoring of our geo-redundant core network.
- Core network – Delivers secure redundant routes to multiple networks in every country to eliminate local coverage gaps.
- Worldwide SIM – Dynamically identifies the best network options in real-time with access to 600+ partner networks in 190+ countries.
- Management Platform – Improves operations and cost controls by providing a consistent experience and unified view of Sierra Wireless SIMs and devices.

The Sierra Wireless SIM has a patented embedded agent that dynamically identifies the best network options available in real-time with multiple routes to multiple networks in every country. This multi-IMSI, multi-network feature is referred to as Smart Connectivity Advanced.

Figure 6. *Sierra Wireless Smart Connectivity service elements, with Ready-to-Connect*


SMART CONNECTIVITY
END-TO-END SECURITY
NETWORK OPERATIONS CENTER
Proactively Prevents Service Disruption
CORE NETWORK
Connects to 600+ Partner Networks
WORLDWIDE SIM
Dynamically Identifies Best Network Options
MANAGEMENT PLATFORM
Improves Operations & Cost Control
Global NOC
Ready-to-Connect

Ready-to-Connect: Plug and Play Solution with fully integrated cellular devices

In addition to the components above, Ready-to-Connect offers a plug and play solution. It comes with pre-integrated, pre-tested and pre-secured components, removing many of the difficulties associated with ensuring interoperability and security. The whole is designed to reduce complexity at every point in the IoT stack - from device to Cloud to central IT system. Of all the steps involved in an IoT deployment, the task of integrating all the components of the solution is often the most complex and time consuming.

Further, the 'Ready-to-Connect' modules, gateways and routers provide instant access to the Smart Connectivity service, thereby simplifying IoT development. They enable a tightly integrated and secure data stream to the Cloud, while eSIMs pre-integrated inside the Ready-to-Connect devices can be activated over-the-air anytime, anywhere, reducing the need for individual device provisioning and reducing gaps where errors can arise.

Wireless Gateways consist of dedicated hardware appliances or software programs and serve as a connection point between the Cloud server/application and the devices and/or sensors. Sierra Wireless' Gateways guarantee a very secure connectivity. They pre-process the data package before sending it to the Cloud; in addition to collecting the desired patient data, they collect data on device and machine status and location.

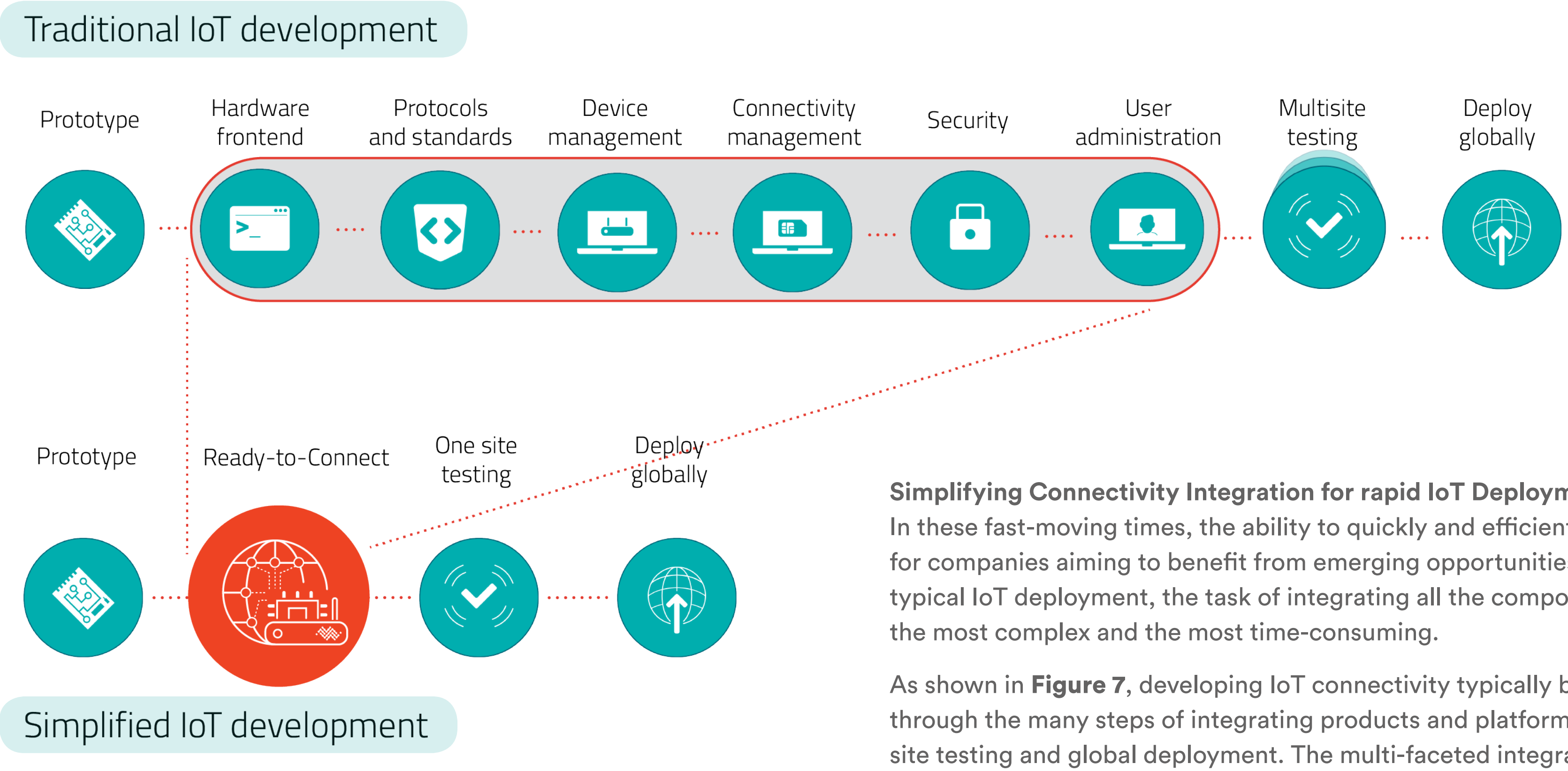
Secure from the Device to the Cloud

To address device security, the concealed eSIMs in the Ready-to-Connect modules prevent SIM tampering or theft, along with the latest encryption technologies in the device, network, and cloud to create layers of protection for the deployment.

One Point of Accountability and Management

The One point of Accountability feature provided lowers the time it takes to identify the root cause of any anomalies or outages in the connected device. High levels of security are needed in order to ensure there is no interference with data transfer and the Sierra Wireless solution provides an intrinsic end to end view of security across the entire production chain. Ready-to Connect uses a layered approach with different security mechanisms built into every component of the solution (device, network, cloud), along with end-to-end schemes, thereby ensuring the appropriate level of security. It also provides a single point of responsibility for the overall security solution. These various security measures work together to protect the deployment, minimise the risk of any loss or theft, and significantly reduce the financial risk of running an IoT-enabled service.

__Figure 7.__ Simplifying connectivity integration with Sierra Wireless Ready-to-Connect



Simplifying Connectivity Integration for rapid IoT Deployment

In these fast-moving times, the ability to quickly and efficiently launch new services is critical for companies aiming to benefit from emerging opportunities. Of all the steps involved in a typical IoT deployment, the task of integrating all the components of the IoT solution is often the most complex and the most time-consuming.

As shown in **Figure 7**, developing IoT connectivity typically begins with prototyping, moves through the many steps of integrating products and platforms, and is then followed by multi-site testing and global deployment. The multi-faceted integration phase is where all the IoT elements come together. It can be a challenging exercise since any issues of interoperability can be costly to address and time-consuming to fix after solution roll-out.

Sierra Wireless' Ready-to-Connect Solution lets IoT teams skip many of the complicated, time-consuming steps commonly associated with the integration phase. The solution includes pre-connected modules and routers, equipped with an integrated global eSIM, and works with the Sierra Wireless IoT Platform to securely manage devices, connectivity and application data.

Key management challenges

Businesses are becoming more reliant on their IoT connectivity as services evolve, with greater emphasis on overall cost reductions as well as increasing revenue expectations. It is one thing to select the most appropriate IoT connectivity to fulfil the needs an IoT project, quite another to manage it in the field. This is especially the case where the applications to be connected are already business-critical or likely to become so.

Beecham's survey of enterprise users and product manufacturers identified four key management challenges:

Managing multiple vendors, where 69% of respondents considered this to be quite or very challenging.

Reducing TOC and BPM cost, where 78% considered this to be quite or very challenging.

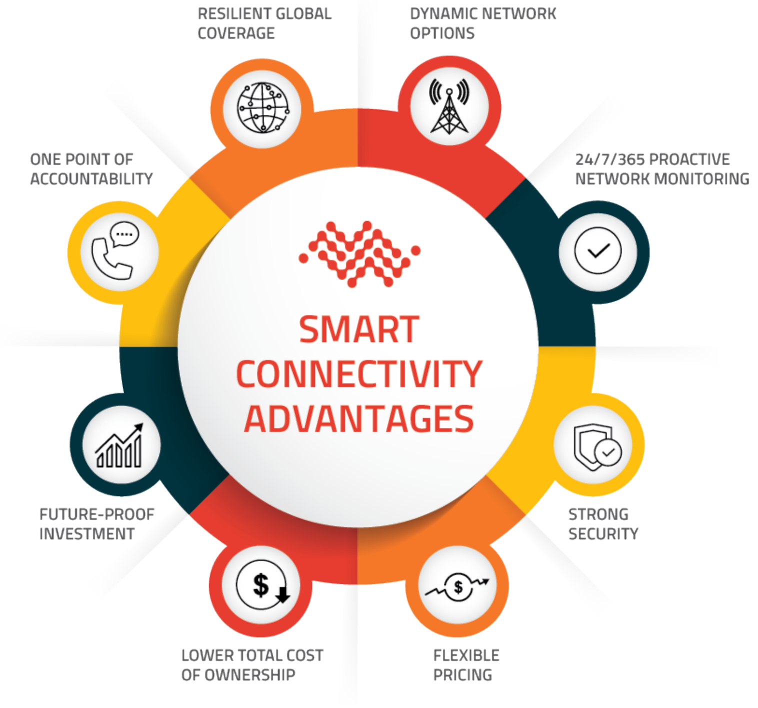
Scaling globally, where 80% considered this to be quite or very challenging.

Reducing time to market, where 66% considered this to be quite or very challenging.

Faced with these significant challenges, Sierra Wireless offers its Smart IoT Connectivity suite, offering major advantages as shown in **Figure 8**.

Sierra Wireless simplifies connectivity choices by delivering the device, software and service solutions needed to accelerate IoT deployment. Innovative products, solutions and services connect thousands of businesses to critical data and millions of people to information. The company remains focused on developing leading technology solutions and on empowering businesses and industries to transform and thrive in the connected economy so they can reduce complexity and turn data into intelligence in increasingly business-critical situations.

Figure 8. *The Advantages of Sierra Wireless' Smart Connectivity offering*


RESILIENT GLOBAL COVERAGE
DYNAMIC NETWORK OPTIONS
ONE POINT OF ACCOUNTABILITY
24/7/365 PROACTIVE NETWORK MONITORING
SMART CONNECTIVITY ADVANTAGES
FUTURE-PROOF INVESTMENT
STRONG SECURITY
LOWER TOTAL COST OF OWNERSHIP
FLEXIBLE PRICING