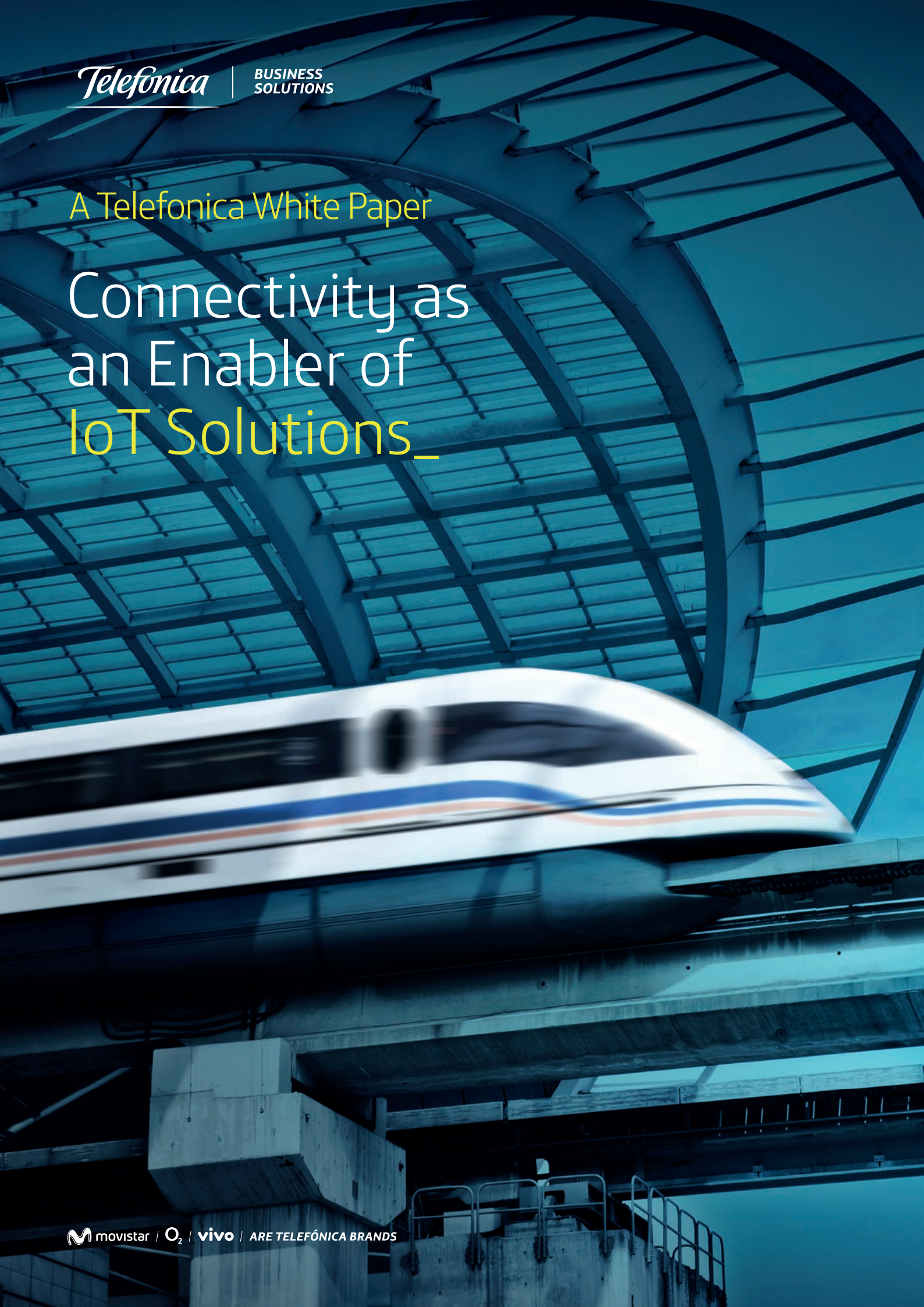


Telefónica | BUSINESS SOLUTIONS

A Telefonica White Paper

Connectivity as an Enabler of IoT Solutions_

movistar | O2 | vivo | ARE TELEFÓNICA BRANDS

IoT market potential

According to Gartner (1), endpoints of the Internet of Things will grow at a 31.7 % CAGR until 2020, reaching an installed base of 20.8 billion units.

In the business segment, the building or facilities automation category, will present the highest growth (a CAGR of 91.6 %) followed by the energy category (CAGR of 81.5 %) and the automotive category (CAGR of 77.6 %).

All this huge growth in the IoT industry brings a wide set of new challenges for customers and to face them the IoT Connectivity Hub solutions are key.

IoT Connectivity Hub

Carriers and OTT vendors have typically deployed managed connectivity platforms delivered as cloud services with different levels of integration into a carrier's networks.

The functionalities of managed connectivity can be accessed via web portal or APIs and include: SIM inventory, SIM life cycle control, alarms and business rules, reports...

Now providers are evolving their value proposition delivering not only basic managed connectivity services but also they are providing a wide set of new advanced services creating a new product category in the IoT ecosystem. The Connectivity Hub category.

IoT Connectivity Hub is an important element of many Internet of Things solutions. It allows the management and automation of customer processes for their connected machines whilst minimizing security and fraud risks.

> "IoT Connectivity Hub can improve customers' productivity, lower costs, increase security and help to expand into new markets or develop new product offerings".

(1) Source: Gartner, Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2015, IoT Units Installed Base by Spending Center, Category and Subcategory, 2013-2020 (Millions of Units) (October 2015)

What are the benefits of IoT Connectivity Hub to a business?

IoT Connectivity Hub can improve customers' productivity, lower costs, increase security and help to expand into new markets or develop new product offerings.

To increase productivity, Connectivity Hub solutions allow a quick and easy integration of m2m services into customer processes and systems using APIs. The functionalities are also available through a web portal accessible from most common web browsers which, in turn, enhance customer experience. IoT Connectivity Hub solutions offer different schemes of SIM lifecycle status models to accommodate them within customer product lifecycle.

In order to assure high availability standards across the connectivity, most service providers use a separate redundant infrastructure from their traditional business for the m2m communications. Some providers also offer global SIMs with extended coverage capabilities.

To lower customer costs, IoT Connectivity Hub solutions offer a wide set of tools to automatically control costs associated with SIM traffic, operation, maintenance and inventories.

To help facilitate the opportunity of tapping into new market opportunities, IoT Connectivity Hub solutions can allow the seamless extension of products and service capabilities into different markets and can even enable new business models by developing new products and services in these new ventures.

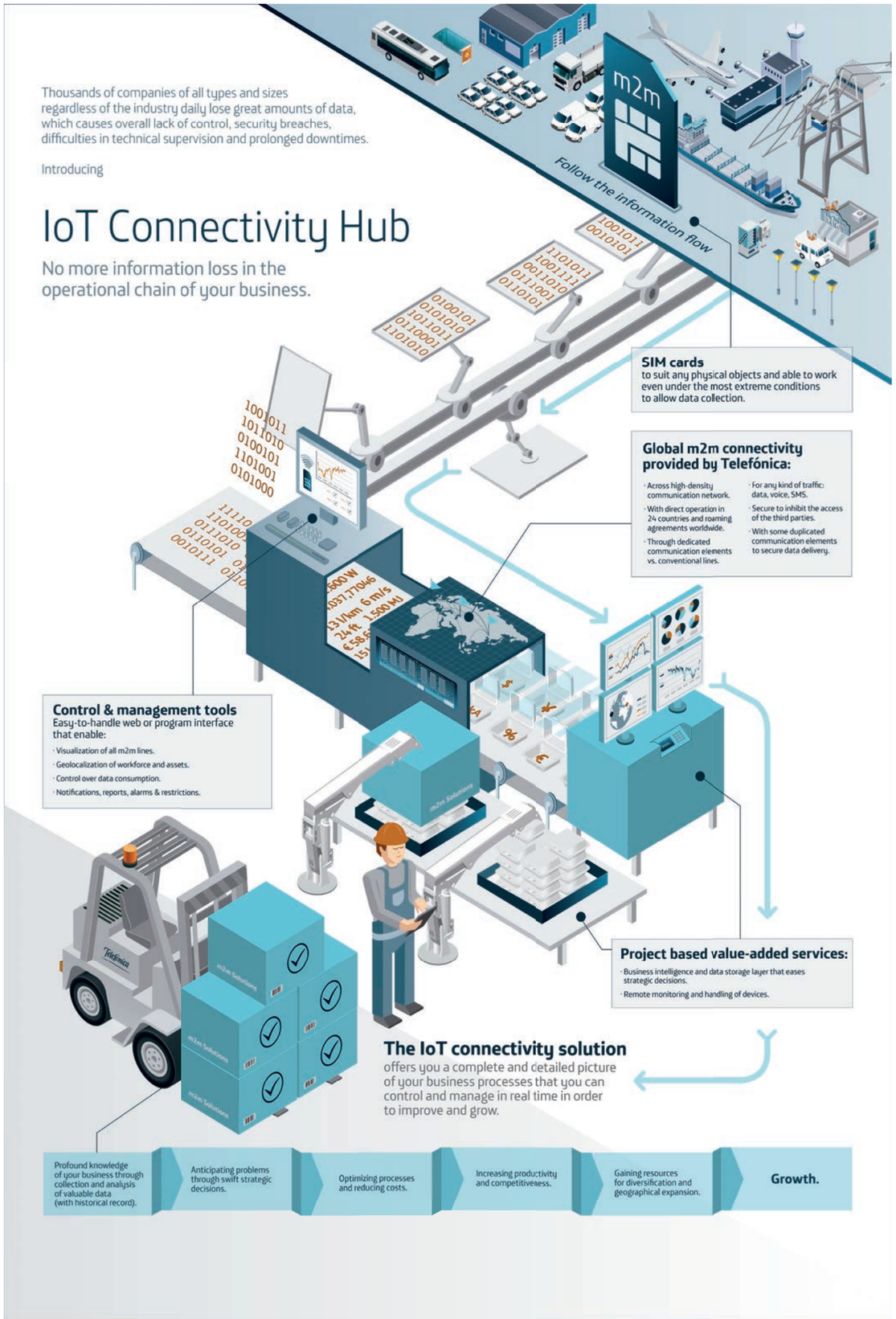
Also, it is well documented that IoT suffers a growing number of cyber security attacks. IoT Connectivity Hub can help minimize these security threats.

Thousands of companies of all types and sizes regardless of the industry daily lose great amounts of data, which causes overall lack of control, security breaches, difficulties in technical supervision and prolonged downtimes.

Introducing

IoT Connectivity Hub

No more information loss in the operational chain of your business.



The importance of finding the right IoT Connectivity Hub solution

Customers' needs are evolving in parallel with the IoT industry boom and that's the reason why current IoT Connectivity Hub solution providers need to evolve their current functionalities portfolio to stay in the game.

Moving to real-time billing

Many IoT customers manage a vast number of SIM cards making traffic across several countries whilst using a heterogeneous and not always up to date portfolio of devices. Sometimes unexpected errors may begin to occur and devices can start behaving abnormally with non-desired calls or data sessions triggering unwanted spending.

Customers want greater billing transparency to minimize the risk of getting a nasty bill shock. To create a truly effective spend limit, the account balance must be monitored and billed in real time. This allows customers to detect when the limit is reached and to take the appropriate action, e.g. suspend the service or send a warning SMS. This is not possible with traditional batch billing and charging.

One of the most regularly demanded features in new connected cars is the need for Wi-Fi Hotspots. This feature allows the car to operate as a Wi-Fi hotspot itself, sharing a wireless internet connection with other devices in the car. For this feature to work, it is critical to control and cut off traffic when customer credit expires. This is only possible with real time billing and traffic control.

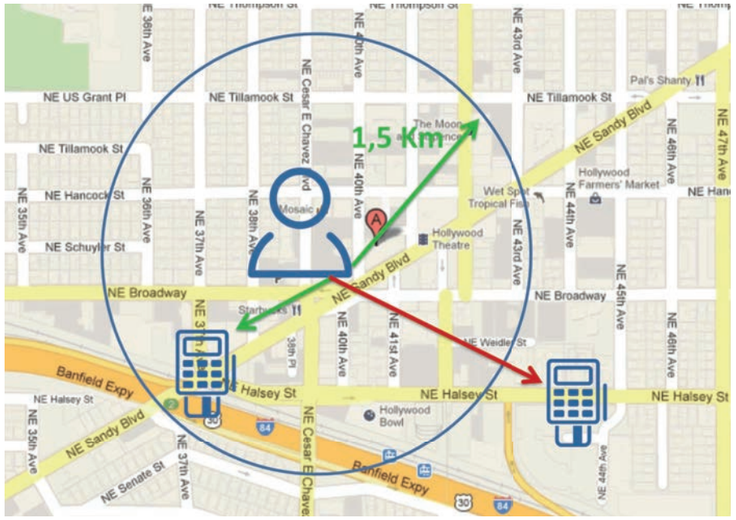
Including location tracking and alarms services

Location services are very useful to customers because they allow the prevention from non-authorized use of the SIM card when the SIM is moved from its typical operations geographical area.

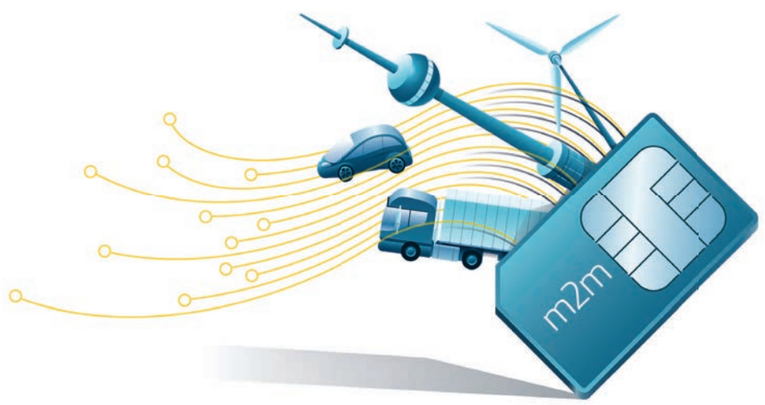
This feature is really valuable for POS business customers, such as restaurants, where it is used to deactivate the SIM automatically when a POS terminal changes its location.This functionality is also relevant in Smart Cities since the devices which are used typically do not change their location.

Location services can increase the efficiency of customer maintenance operations. Most IoT customers have large deployments of SIMs distributed over large geographical areas. IoT Connectivity Hub solutions allow customers to integrate the location information via API to their operation systems and to manage the optimal routes to facilitate on-field tasks.

The location services provided by IoT Connectivity Hub solution providers are based upon cellular network cell-id information together with alarms and automatic business rules. This allows business rules to be automatically actioned when a change in location is detected, such as deactivation of services or notifications.



> "IoT Connectivity Hub solutions allow customers to integrate the location information via API to their operation systems and to manage the optimal routes to facilitate on-field tasks".



Taking care of security since it is critical for IoT solutions

Recently, there have been numerous IoT security-related scandals and it is clear that IoT is becoming an increasingly attractive target for cybercriminals.

A recent demonstration by two researchers at Def Con Hacking Conference where they showed the ability to control the steering, braking and transmission of a connected car, led to the recall of 1.4 million vehicles in a bid to install a security update. This clearly served as a huge wakeup call to the IoT industry and highlighted the requirement to increase security levels.

Making huge steps in new technology innovation is often accompanied by misuse and those looking to make abuse these new advancements. It is now more evident than ever that IoT will only be successful if the industry manages to secure the solutions that they build.

The biggest risks in IoT security come from within the devices themselves, as well as from the platforms that support these devices. Many of the devices are built on top of open source libraries and components and device manufacturers are continuously updating their firmware as they find vulnerabilities. IoT Connectivity Hub is a key component to increasing these security levels in IoT solutions and help prevent security attacks and fraudulent uses.

Each IoT market segment requires different levels of security. For instance, the connected car sector or eHealth sector requires many more security features than agriculture.

There are several IoT connectivity Hub features to prevent security breaches that can be grouped in multiple layers:

Connectivity / transport security:

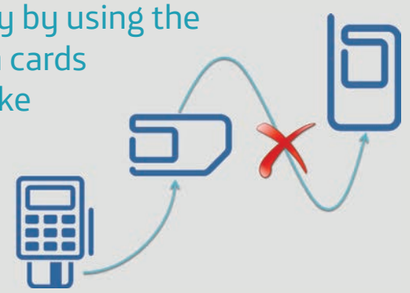
- **Private APNs and secure connectivity.** Most IoT connectivity Hub providers offer a wide set of different connectivity choices to connect devices according to their security needs:
  - Internet
  - Internet with IP filters
  - IPSec
  - MPLS

Platform security:

- **All infrastructure that supports the service has to follow the highest security standards.** Telco players usually includes security capabilities within their own networks, like dedicated IoT infrastructure and redundancies, in order to prevent against external attacks.
- **Secure customer access to the web portal and APIs** in which customers can manage the SIMs. To improve security some platforms can provide customers with **https, certificates and even two-factor authentication processes.**
- **Profile management.** Customers can manage several profiles over the same account to guarantee that each employee accesses to the information that is relevant for his or her role.
- **IMEI change alarms and automatic business rules** to ensure the SIM only can be used in an authorized device, blocking its use in other devices. The automatic business rules include notifications, activation/deactivation of services and updates of SIM status.

Did you know

400 high-tech South African traffic lights were put out of service after thieves in Johannesburg stole the m2m cards they contained. The thieves spent huge amounts of money by using the stolen cards to make calls.



> **Numbering restrictions to outgoing and/or incoming calls and SMSs.** IoT Connectivity Hub solutions allow the ability to block all outgoing and incoming calls with numbering rules that can be customized by the customer.

> **Service activation/deactivation at SIM level.** Customers can autonomously manually activate or deactivate services at SIM level. This is relevant in some industries in which device firmware is configured by SMSs. Customers can only activate SMS service during maintenance works.

> **Real time control of traffic and expenses.** Customer can establish thresholds for the traffic and expenses at SIM level taking into account their typical device traffic needs and get notifications and trigger automatic actions when they are reached. This minimizes unwanted impacts since customer can react without delays.

> **Location change alarms and automatic business rules** to ensure that the SIM can only be used at its typical authorized location. If somebody moves the SIM to another location an automatic action can be configured to deactivate the SIM or to make a notification.

Customer application backend security:

> **Vulnerability management service** to detect the weak points of customer backend application, identifying corrective or preventive measures.

IoT Device security:

> **Use certificates and public keys infrastructure for strong device authentication providing digital identity** to any IoT device, allowing added value services such as digital signature and the ciphering of sensitive data stored in the device.

Future trends in IoT Connectivity Hub solutions

IoT solutions are growing in complexity often using different approaches to provide connectivity.

The technologies that are currently available to cover the connectivity layer of the IoT solutions are:

> **Traditional Cellular (2G, 3G, 4G)**

> **Cellular Low Power Wide Area (e.g. Sigfox)**

> **Mesh (e.g. ZigBee, Z-Wave, etc.)**

> **Fixed Line**

> **Satellite**

> **Wi-Fi**

Customers are deploying solutions that use, under the same service, a diverse range of devices each requiring different types of communication, and want to manage all of these together under a single unique managed communication service.

This business need for the control of a unique manage communication service is the reason IoT Connectivity platforms are evolving to act as a central connectivity hub for this new arena.

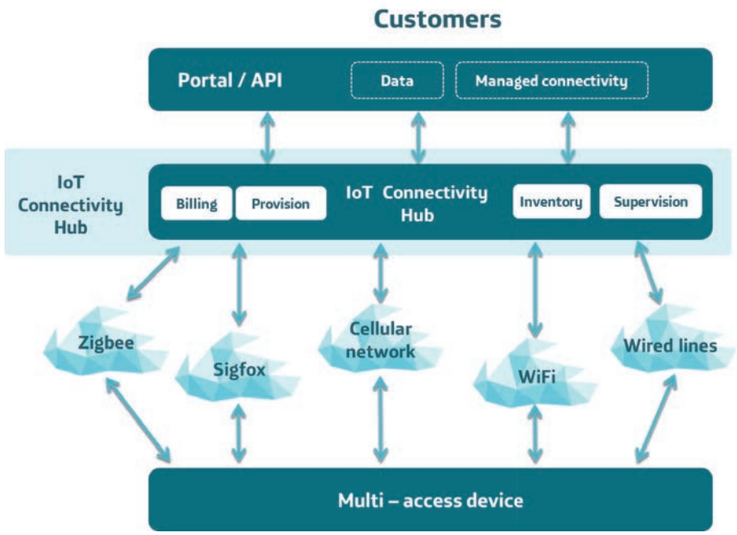
IoT Connectivity Hub solutions are also growing in the IoT end-to-end value chain since they are including device management capabilities. These new features are:

> **Device inventory**

> **Device auto-configuration**

> **Device software and firmware updates management**

> **Remote diagnosis and error fixing tools**



Telefonica IoT Connectivity Hub: Smart m2m

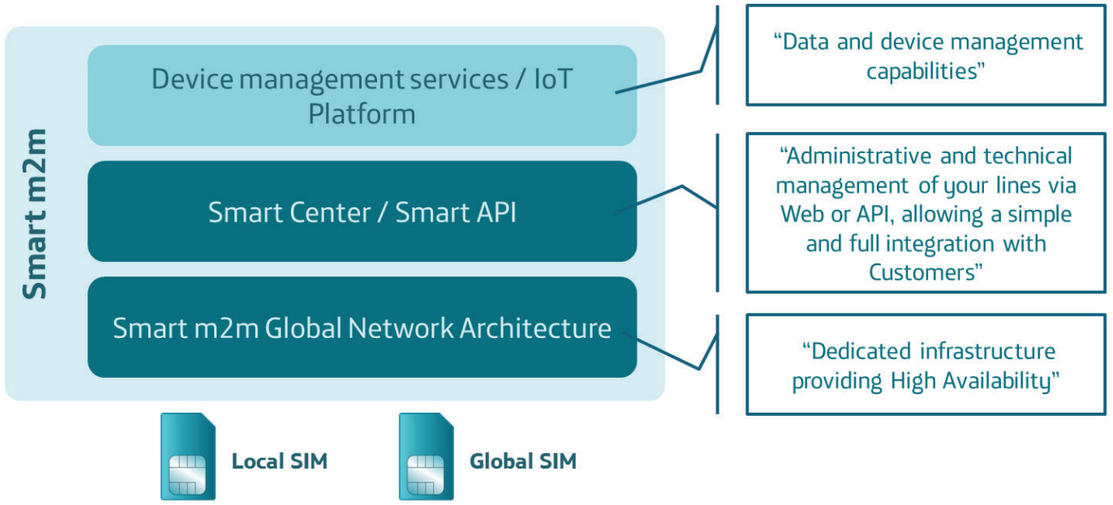
Smart m2m is an IoT Connectivity Hub solution developed in-house by Telefonica, currently with more than 1,000 customers globally distributed.

Smart m2m is designed to have all the typical managed connectivity services (Inventory, SIM life cycle control, alarms and business rules, reports...) and furthermore a set of differentiating features such as:

- **Real time billing control**
- **Geo location services**
- **Device management capabilities**
- **Enhanced security features such as:**
  - Physically and environmentally redundant and secured infrastructure
  - Location detection changes alarms
  - Numbering restrictions to outgoing and/or incoming calls and SMSs
  - Service activation/deactivation at SIM level
  - Vulnerability management service
  - Digital identity service

Allowing Telefonica to provide customers with an end-to-end security IoT value proposition to prevent, detect and respond to any potential risk.

All advanced and standard functions are accessible via secure web portal or API.



About Telefonica Business Solutions

Telefonica Business Solutions, a leading provider of a wide range of integrated communication solutions for the B2B market, manages globally the Enterprise (Large Enterprise and SME), MNC (Multinational Corporations), Wholesale (fixed and mobile carriers, ISPs and content providers) and Roaming businesses within the Telefonica Group. Business Solutions develops an integrated, innovative and competitive portfolio for the B2B segment including digital solutions (m2m, Cloud, Security, e-Health or Digital Marketing) and telecommunication services (international voice, IP, bandwidth capacity, satellite services, mobility, integrated fixed, mobile, IT services and global solutions). Telefonica Business Solutions is a multicultural organization, working in over 40 countries and with service reach in over 170 countries.

For more information, **visit business-solutions.telefonica.com** or our dedicated IoT website: **iot.telefonica.com**

	@TelefonicaB2B	**@Telefonica IoT**
YouTube	**Telefonica Business Solutions**	**Telefonica IoT**
in	**Telefonica Business Solutions**	**Telefonica IoT**