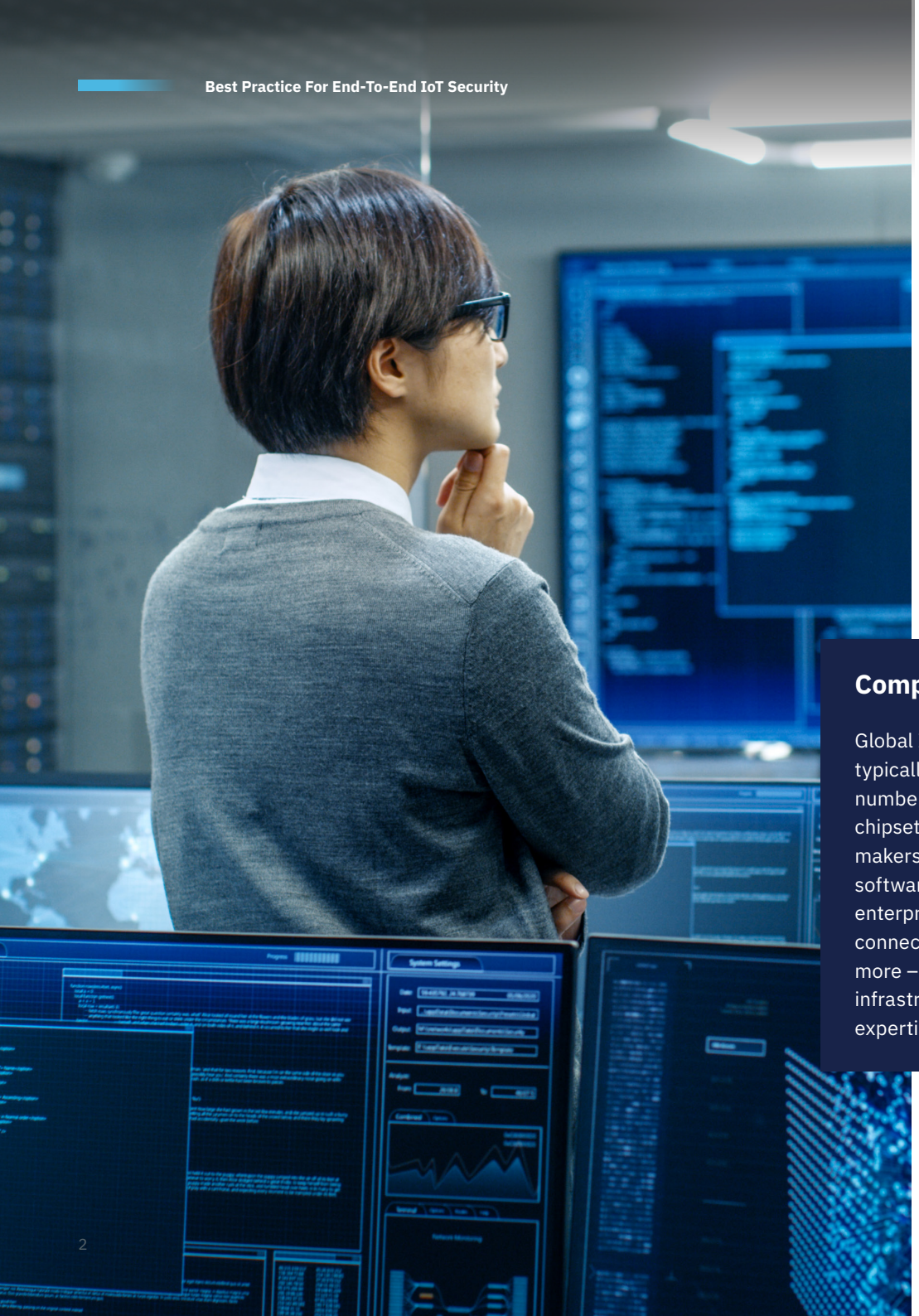
bics

# Best Practice For End-To-End IoT Security



# Introduction

Security concerns remain a major barrier to IoT adoption for as many as 85% of IoT industry leaders[1]. Fraud is growing in this area, causing widespread agreement across the ecosystem that securing the IoT application is the only way to fully develop its business potential. The good news is the vast majority of attacks can be prevented – and the resilience of any IoT deployment significantly improved – with measures that are simple and cost-effective to implement.

This white paper explains how mobile connectivity is a central enabler of IoT security. It outlines best practice advice for protection built in at each layer of an IoT solution, and at every stage of its development.

## IoT security can appear extremely complex at first sight

Most IoT projects today are based on complex ecosystems, involving numerous players and covering a range of use cases across multiple access technologies.

### Complex ecosystems

Global IoT deployments typically involve a large number of players, including chipset manufacturers, device makers, systems integrators, software platform providers, enterprise back-end systems, connectivity providers, and more – all with differing infrastructures, profiles, expertise, and experience.

### Diverse deployments

Compliance and common standards across all stakeholders must be both strong and flexible because every vertical has its own specific needs and nuances. The security requirements for a smart building, for example, are very different to those of a payment terminal.

### Infinite applications

Global IoT deals with mass and diversity; it has to scale to accommodate hundreds of thousands of devices and device types with completely different life expectancies, criticalities, storage, and processing capabilities.

As a result of this diverse ecosystem, a unified global security standard and certification for IoT is lacking today, even though there has been progress in certain areas.

[1] Omdia and IoT World Today, 2020

# The IoT attack surface

## All IoT deployments follow a three-layer framework

**The device layer**
This consists of the physical device – software, hardware, and connectivity ports.

**The network layer**
This carries the data between the device and the application layer. There is usually an access network – either WiFi, mobile or fixed – and a transport network that can be public internet or a private network.

**The application layer**
This manages the data generated from the connected device, including the provision of some control and authentication when required.

Every IoT layer is exposed to different risks. This creates a broad range of threats, from data interception and impersonation to location tracking, denial-of-service, and service frauds. Adoption of basic security measures and protection to reduce the attack surface at each layer can have a huge impact on the overall level of deployment security.

A complete and comprehensive end-to-end strategy is essential. Adopting a security-first mindset during planning, buildout, and operation will ensure the greatest impact at the lowest cost.

# Ensuring end-to-end security during the design, build, and launch of an IoT project

## Design stage

Enterprises must adopt a “security by design” approach to identify and address potential threats at the earliest possible stage, when fixes can be implemented most easily. It should encompass devices, connectivity, application platforms, and APIs. **The later in the process, the higher the cost and difficulty of implementing a fix**.

‘Security by design’ starts with a risk assessment, reviewing the service architecture and key components to introduce adequate levels of confidentiality/ encryption, integrity checks, authentication, and accreditation. These parameters can also be used to validate third party compliance during the selection process.

At this stage, a key connectivity consideration is to segregate data transmission from the internet. Organizations can limit which servers a device can interact with, and define volumes or throughput thresholds. They can also control the mobility pattern or profile to be activated for their devices at the network level. Depending on the criticality of the application and data, operational solutions such as a firewall or intrusion detection system should also be considered.

## Build stage

During the build stage, penetration tests and reverse engineering are essential to validate that the security of the solution is in line with the requirements, and to identify vulnerabilities. Tests must include not only security of data “at rest”, but also “in transit” over the network. Penetration testing should be conducted against each layer, as well as on the overall deployment.

A complete set of best practice guidelines is available from the GSMA to help companies build their IoT deployments with end-to-end security. These reference documents provide a comprehensive set of verifications, checkpoints, and considerations to evaluate the security of their projects.

## Launch stage

The key focus here is maintaining the integrity of the deployment over time by creating and maintaining security in change management and operational processes. Recurrent penetration testing by third parties is useful to validate security after a given period, or to test against new threats.

For mission-critical deployments, real-time monitoring solutions such as intrusion detection systems can be added, along with firewalls. Automation, big data analytics, and machine learning must be used to bring scalability, pattern recognition, and profiling capabilities.

Whether consumer applications or industrial M2M, data security is critical to the long-term success of IoT. Security must be a concern of every player in the value chain, and enforced on the device, network, application, and across the three layers at each stage of development.

# Best practice for securing IoT connectivity

Connectivity sits at the center of the technical chain of any IoT project, and so the way in which devices are connected to the IoT application server represents a key security consideration.

## The central position of connectivity is beneficial in two ways:

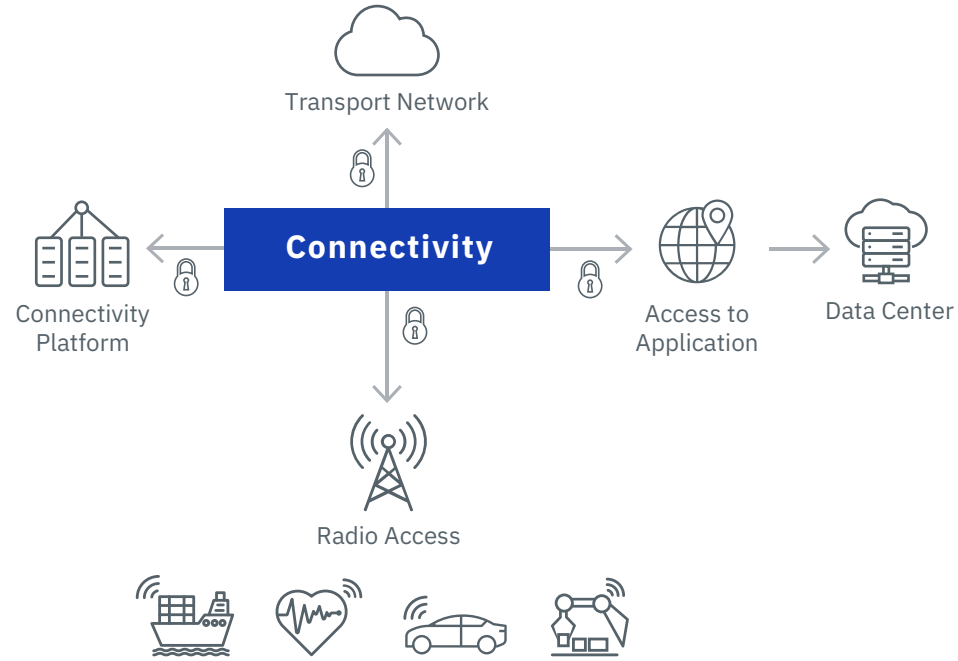
1. It can play a central role in actively securing the end-to-end IoT solution:
   - Detecting any abnormal or malicious data getting in or out to/ from the device and to/ from the application
   - Filtering and blocking malicious traffic
   - Allowing monitoring and control across device traffic, including IP traffic and signaling traffic

2. It can be designed to withstand intrusion, protecting the end-to-end solution and ensuring segregation of critical traffic

## End-to-end, connectivity follows a technical chain made up of four steps:

- The radio access for the device
- The transport network to the connectivity platform
- The connectivity platform itself
- Access to the data center where the application is hosted

To secure connectivity at each step of the technical chain, enterprises must take into consideration the following five guidelines.




## 1. Select the right radio access technology

**Mobile technologies (2G/ 3G/ 4G/ 5G/ LTE-M/ NB-IoT) hold a clear advantage for IoT:**

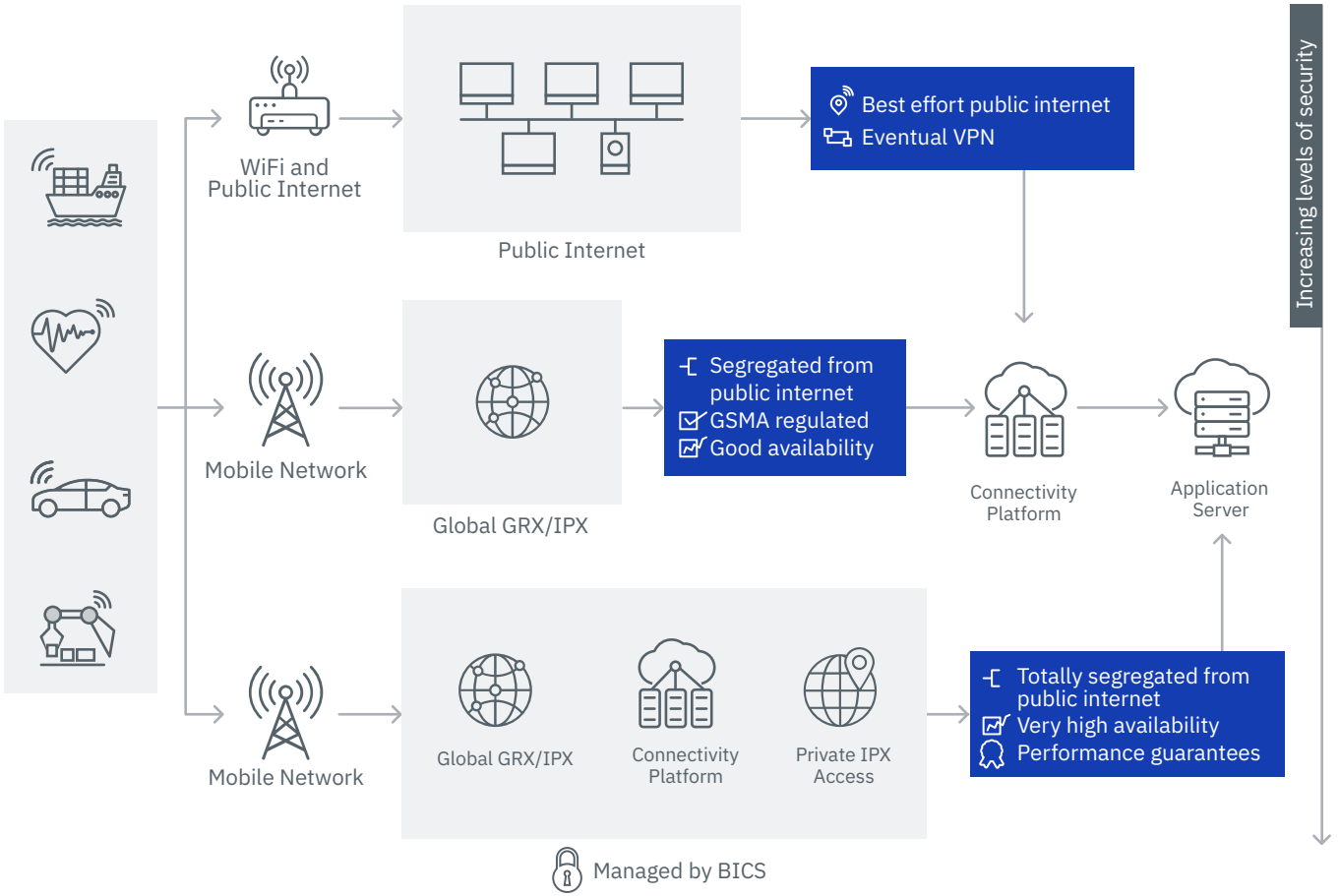
- Availability is unmatched by any other radio technology, as mobile networks are ubiquitous around the world
- A SIM card ensures the highest security in authentication
- Radio encryption of mobile networks has been guaranteeing the integrity of communications for more than 25 years

## 2. Segregate the flow of data from the public internet

**Segregate the flow of data between the transport network and connectivity platform from the public internet.**

Compared to WiFi networks that always break out to the internet, mobile networks have a strong advantage. In international roaming scenarios, mobile data traffic uses a highly secure infrastructure called GRX/ IPX, standardized and governed by the GSMA.

This means that when a 2G/ 3G/ 4G/ 5G/ LTE-M/ NB-IoT device is connected abroad to a visited network, all the data is carried securely on a private network to the connectivity platform.



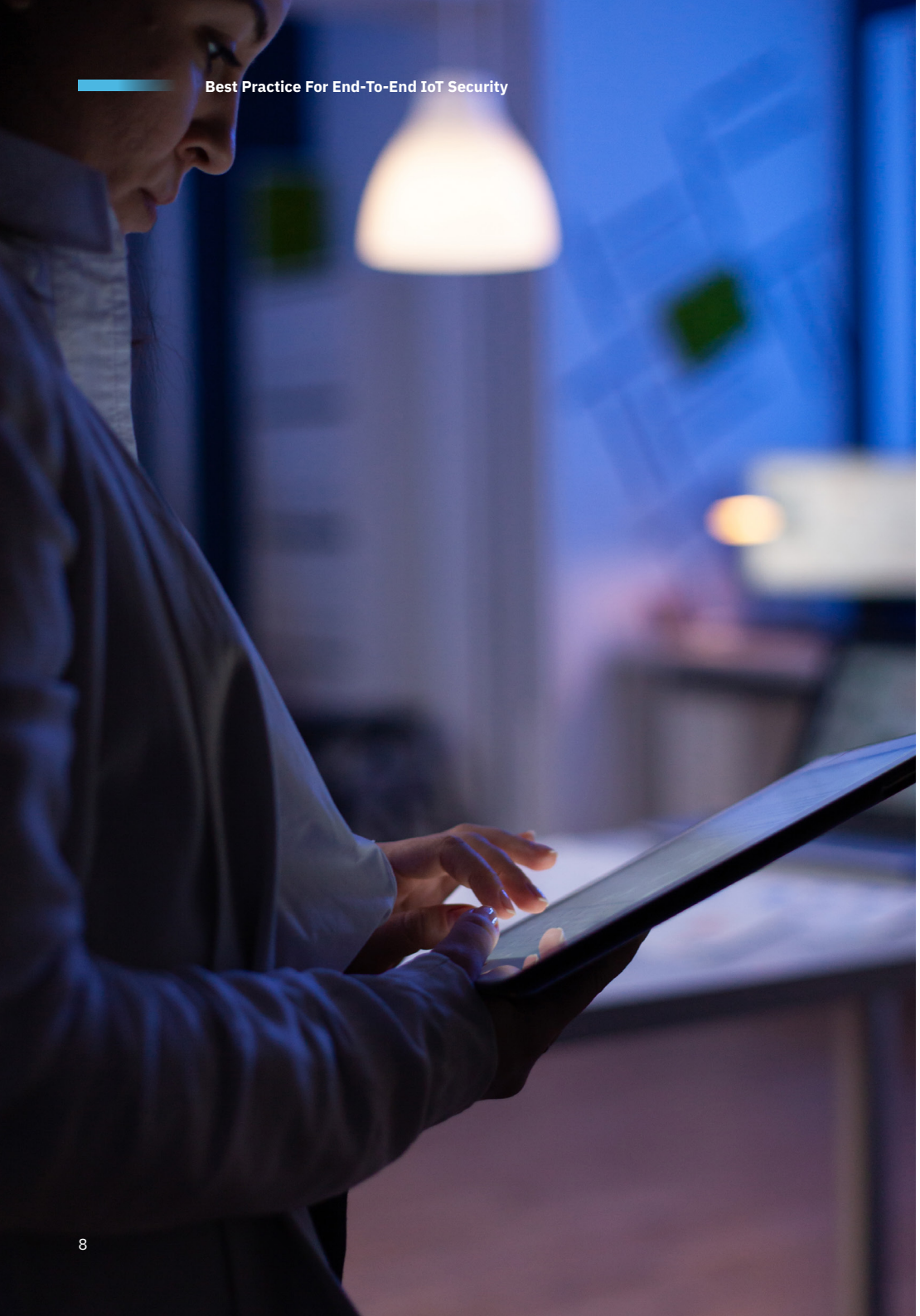
## 3. Opt for a private IPX to reach the application server

When accessing the application, best practice for security is to again segregate data flow from the public internet. This can be done by using a private IPX, thus extending the security of traditional GRX/ IPX up to the application server.

Security risks always grow with the number of players involved in connectivity: each interface is an opportunity for external attacks. A consistent policy across the technical chain is a must-have for effective management of these risks.

Some international carriers act as global MVNOs for IoT, which puts them in a unique position to control the connectivity from the visited country up to the data center of the enterprise. This approach is a strong guarantee of consistent end-to-end management of security.

For a number of IoT use cases, it is also possible to differentiate the data traffic into two parts: non-critical (such as web surfing) and critical (for example, all device, application, and customer management data). This can be achieved with a connectivity provider that can manage various APNs with different routing management; noncritical data traffic is broken out to the public internet, while critical data traffic is routed over the leased line or private IPX. This allows the enterprise to optimize budget, while ensuring a high level of security for their critical applications.



## 4. Assess security of the mobile core network and resiliency of connectivity

Over the years, multiple cases of network exploitation have been disclosed where international signaling was used as a means of attack, such as denial-of-service, SMS interception, and location tracking.

To protect their infrastructure and subscribers from these activities, connectivity providers must assess network protection on a regular basis and implement technical solutions, such as signaling firewalls, to proactively detect and block such attacks. They must also ensure full redundancy of their connectivity platform and have a disaster recovery plan in place.

For international projects, end-to-end connectivity is more complex, and providers must be able to connect devices securely and reliably in all required markets, which usually means:

- Having at least two mobile operator partners in every country
- Being able to reroute data roaming (GRX/ IPX) and roaming signaling if outages occur

## 5. Deploy a smart connectivity platform

The role of the connectivity platform is to manage the connectivity of each device across all networks, including the traffic in and out. Intelligence can then be set up inside this connectivity platform to protect devices and the application server, such as:

- **Detection of abnormal behavior.** The majority of IoT applications follow very clear patterns of use. For example, if a device that is supposed to send a report of 1 MB once per week starts sending more data or more often, this can be an indication of malicious activity.
- **Geofencing.** Network-based geolocation is the only geolocation technology that cannot be spoofed. The platform can use information that is 100% reliable to determine which base station each device connects to.
- **Fraudulent use of SIM cards.** If a SIM is removed from the IoT device and placed into a smartphone for personal use, the connectivity platform can detect this and automatically block the SIM card.
- **Network firewalls, such as filters on URLs, IP addresses, etc.** This will only allow traffic for specific destinations and/ or applications.
- **Deep packet inspection (DPI).** This can be used to detect abnormal content in data flow.

# Conclusion

**As the number of deployments soars, IoT security has never been more critical. With every innovation comes the opportunity for a more sophisticated means of capitalizing on its weakness. Sat at the heart of each IoT deployment, connectivity plays a central role in protection. Here, mobile technologies offer unique advantages.**

The mobile industry is also constantly creating standards for connectivity with a strong focus on security, thus significantly increasing the protection of mobile subscribers and connected devices. 5G standards and specifications perfectly illustrate the trajectory of security by design, integrating enhanced and reinforced radio encryption, authentication, and integrity, alongside mechanisms specifically designed for IoT.

When selecting a global mobile connectivity provider, enterprises must look carefully into three main aspects:

1. Intelligence of their connectivity platform to detect abnormal behaviors and act against potential security risks.
2. Quality and reach of their global IPX infrastructure so that all solutions, from device to application, remain securely connected regardless of location.
3. Design of their solution to ensure protection from external attacks, such as through international signaling.

By working with mobile operators or mobile virtual network enablers, enterprises can leverage a global, robust, and secure infrastructure already in place, complete with ever-improving industry standard security processes and best practice at every stage of connectivity. Enterprises must also consider tapping into the security and reliability of IPX networks that the mobile community has been able to deploy globally for the past two decades.

For more information, please visit:
**www.bics.com**