JT IoT

# QUICK GUIDE TO IOT

## Are your IOT SERVICES secure?

JT Group Ltd

@JT_business

www.jtiotsims.com

# Are your IOT SERVICES secure?

## Are you confident that you're protected?

**Businesses are rushing to take advantage of the opportunities that IoT services can unlock.**

IoT solutions enable the collection of rich new sources of data from remote devices, deliver new, granular tracking capabilities, and enable advanced remote control. This data exchange is facilitated by mobile networks.

This means IoT services need to be completely secure, so that businesses can be confident that they are protected from threats, vulnerabilities and incursions. They need peace of mind, so that they can capitalise on the benefits that IoT services and applications can deliver.

## Security is essential for successful IoT services

**IoT services extend enterprise boundaries into a growing number of field locations.**

You need to control your devices at the same time as collecting valuable data from them. This means that they need to be protected, just like any other enterprise IT asset.

So, for your IoT services and applications to succeed, you must be sure that they are protected. It's not enough to simply connect across a network, additional precautions must be taken. You need an IoT connectivity provider that includes stringent security as part of their service offer.

## What are the key IoT Security risks?

**IoT services can be vulnerable across several dimensions.**

First, because of the sheer volume of devices that businesses may deploy, the overall attack surface will increase. With more devices, there are more points to attack and so scale itself becomes a vulnerability. The more you deploy, the more there is to attack.

Second, there are typical IT threats, such as malware, DoS attacks, as well as bots, which are targeted at devices, which can be hijacked.

Third, because IoT services must be delivered across a wide area network (WAN), there are also other vulnerabilities, such as direct attacks on the signalling network that conveys the IoT data. Collectively, these are known as attack vectors

> "You need to control your devices at the same time as collecting valuable data from them. This means that they need to be protected, just like any other enterprise IT asset."

JT IoT

## What do you need to secure your IoT services?

**An IoT service or application must be protected, at the level of both the attack surface and the attack vector.**

For IoT services that connect across mobile networks, this means you have to consider both the network and the devices. They cannot be viewed in isolation, as each must be protected.

The mobile network must be secured, to ensure that only legitimate messages can flow through it and that malicious messages are detected and eliminated. The attack vectors include devices, the data path for message exchange and the network which enables message delivery. This means that each of these vulnerabilities must be considered and different solutions applied to each.

"For IoT services that connect across mobile networks, this means you have to consider both the network and the devices. They cannot be viewed in isolation, as each must be protected."

**Step 1**
Encrypt messages

**Step 2**
Protect paths

**Step 3**
Use a firewall

## How is this achieved in practice?

**Device-level security can be achieved by deep encryption of messages, making them invulnerable to decryption.**

This protects valuable data and ensures privacy. The next step is to protect the data path, which can be secured by creating private APNs or VPNs. Essentially, this builds a private LAN for your devices, but one which spans the entire deployed footprint around the world. It brings them inside your enterprise border protection.

The mobile network must be protected by what's known as a signalling firewall. This is like any enterprise firewall but is optimised for the unique demands and elements of the mobile network. It provides real-time screening and filtering of suspicious activity and only enables legitimate messages to enter the network.

JT IoT

JT IoT

## How do know your IoT services are secure?

**Businesses need to know what's happening to their IoT services and to understand the scale of any threats, as well as how successfully they have been repelled.**

They need to be alerted to any incursion and to obtain accurate reporting regarding service performance and uptime.

You need a comprehensive management and reporting portal, which provides at-a-glance information as well as real-time alerts and alarms and historic data. It must allow integration with your own systems, providing the peace of mind you need to support your remote IoT services, wherever your devices have been deployed.

## Security checklist - what you need to look for

- Protection for all attack vectors
- Protection across the attack surface
- Private APNs / VPNs
- Public and private IP solutions
- Mobile network firewall
- Deep-level encryption
- Rich reporting, visibility and analytics

## JT – the unique, global IoT connectivity provider

**JT's services are unique, due to the truly global coverage delivered, spanning more than 700 operators and more than 700 roaming agreements.**

Offering the flexibility and agility of an integrator, with the global reach and network control of a Mobile Network Operator, JT has more than 120 years of heritage. We're a strategic asset of the local government, the State of Jersey, so our customers benefit from the security of long-term viability. 18 of the world's top 20 banks depend on our services.

Our platform, NOMAD, offers unique capabilities for building and customisation IoT services, covering connectivity, provisioning, monitoring, and remote diagnose. JT offers the complete IoT stack, providing a robust, secure solution for your IoT service requirements.

JT IoT

JT IoT

JT Group Ltd

@JT_business

www.jtiotsims.com