consoleconnect

The 2024 guide to connecting IoT devices to the cloud

How to build networks that balance security, scalability & performance

Bridging the gap between **device and cloud**

The number of Internet of Things (IoT) devices worldwide is forecasted to almost triple from 9.7 billion in 2020 to more than 29 billion IoT devices in 2030*.

These IoT devices have the ability to gather data, communicate with each other, and provide real-time feedback, making them a valuable resource for businesses and consumers alike.

As IoT device form factors have got smaller and batteries have got better, use cases for IoT applications have expanded into every sector.

From trucks, to shipping containers, people, to cattle, an organisation's assets can be fixed, mobile, autonomous and even sentient - relaying information that can deliver new business insights and competitive advantage.

But these benefits only come if the information is able to get to the right place at the right time. The integration of IoT and the cloud in particular creates the opportunity for a unified IT infrastructure for a company. Organisations linking the two different technologies together will reap the benefits of both and create a convenient way of working.

However, they must be able to accomplish this without additional complexity and without compromising on performance or security.

In this ebook you will learn:

- 3 key considerations when connecting devices to the cloud
- The new security risks presented by IoT growth
- How to better protect IoT devices
- 3 IoT applications that should avoid the public internet
- How Edge SIM delivers security, scalability and performance

*Source: Statista

3 key considerations when **connecting devices to the cloud**

The popularity of cloud computing has made connecting to it mainstream with providers like Amazon now offering their own software tools.

Increasingly connecting IoT devices to the cloud benefits from greater flexibility, more robust disaster recovery, and automatic software and security updates if some pitfalls are avoided.

With multiple devices to connect to the cloud, scalability, flexibility, and network connectivity can become challenging and a setup that works for one cloud and network cannot simply be easily replicated for another setup.

Here are 3 key considerations for connecting devices to the cloud:

1. **Scalability:** The rapid IoT device growth requires cloud platforms to handle large amounts of data from a variety of sources while maintaining performance or reliability. these platforms must be able to scale up or down and expand geographically based on demand, without causing any downtime or interruptions.

2. **Simplicity:** IoT devices are often developed by different manufacturers and with different protocols. Simplifying IoT device compatibility to access a cloud platform or consolidating solutions after the merge or acquisition of 2 different organisations may be tricky. To overcome this challenge, IoT providers must develop universal standards for IoT devices and cloud platforms to ensure compatibility. Industry-wide standards would allow for interoperability between devices and cloud platforms, making it easier for organisations to connect and manage their devices.

3. **Network connectivity:** IoT devices often rely on wireless networks to connect to the cloud. Common connectivity issues in areas with poor signal strength or network congestion are well-known and hard to address. Other less known issues are the traffic path between the wireless networks and the cloud proper.

For example, if an organisation deploys cloud services in the US and wants to deploy the same service using the same cloud in Asia, the cloud is the same, the hardware is the same, but the access network will be different. Failure to acknowledge this implies service repercussions such as data loss, delayed data transmission, or complete device failure.

To overcome network connectivity challenges, IoT solution must built-in end-to-end connectivity diversity with redundancy and backup systems in mind. Additionally, cloud access must have a robust network infrastructure capable of handling large volumes of data and providing reliable connectivity to IoT devices anywhere these devices may be.

The new security risks **presented by IoT growth**

IoT deployments continue to expand globally, revolutionising the way businesses operate by boosting efficiency and enhancing experiences for customers and employees. But as is the case with many innovations, growth has outpaced security considerations resulting in unforeseen problems emerging as bad actors seek to exploit new vulnerabilities.

In a paper by the UK's National Cyber Security Centre, the organisation warned:

- It is highly likely that the growing number of Enterprise Connected Devices (ECDs) being adopted by enterprises presents an expanding attack surface, with many of these devices being accessible over the public internet, and with cyber security often being an afterthought.
- It is highly likely that ECDs will be used as an attack vector or pivot point to enable cyber actors to gain access to an enterprise's corporate network for espionage purposes, disruption, or financial gain.
- Deployments of ECDs present a different threat profile from typical consumer use. Organisations often have more knowledge, responsibility and control of networks and cyber security, compared with a typical consumer.

This is further supported by recommendations in ETSI EN 303 645, which is the European standard for cybersecurity requirements in IoT devices.

One of the key recommendations is to minimise attack exposure surface, meaning - amongst other things - avoiding exposing IoT devices to the internet whenever possible.

Incidents of IoT hacks on the rise

In the past few years, there have been many examples of hackers using the public internet to access IoT devices:

- **Medical devices:** In 2022, hackers were able to hack into insulin pumps and change the settings, which could have resulted in serious harm to patients.
- **Baby monitors:** In 2021, hackers were able to hack into a popular baby monitor brand and watch babies in their cribs.
- **Smart speakers:** In 2020, hackers were able to hack into Amazon Echo speakers and issue commands to turn on lights or lock doors.
- **Internet-connected thermostats:** In 2019, hackers were able to hack into Nest thermostats and change the temperature to freezing.
- **Security cameras:** In 2017, hackers were able to access over 100,000 security cameras around the world.

And the list keeps growing...

IoT growth outpacing security

The implication is concerning, in that security considerations are not keeping up with use cases, as IoT systems begin to have a direct impact on people's experiences in the real world, including the food we eat, the elevators we ride, the traffic we move through, and the medical care we receive.

Part of the challenge is in the applications themselves - IoT devices are also often severely constrained in terms of footprint and available compute and processing capabilities - the result is they often can't support security clients on-device.

The other thing is that to facilitate ease of use and grow adoption, many of these devices connect to the public internet directly with a public IP address - and that goes across the spectrum, from a fresh coffee machine in the corner of a supermarket, to an industrial sensor in a nuclear power station, both of which have very different implication in terms of the disruption of essential business processes or compromise of vital and valuable data.

There are even search engines like Shodan that specialise in trawling the IoT and cataloguing every publicly visible device out there, making it easy for businesses to identify their vulnerable assets, but also opening up the same capability for the bad guys.

How to better **protect IoT devices**

There are a couple of ways to avoid exposing IoT devices to the internet – that in turn help to protect them from cyberattacks:

- One way is to use a local area network (LAN) to connect the devices to each other and to a controller. This way, the devices are not directly connected to the internet and can only be accessed by authorised users. And then if the controller needs to be connected to other cloud-based instances, that connection needs to remain on a private network as well.

- Another way to avoid internet exposure of the device by connecting them directly to the cloud-based instances via fully private networks. In addition, it is important to keep IoT devices up to date with the latest security patches. This will help to protect the devices from known vulnerabilities.

In addition to avoiding internet exposure, the ETSI 403 645 standard also recommends a number of other security measures for IoT devices, such as:

- Using strong passwords and authentication methods
- Encrypting data in transit and at rest
- Regularly scanning for vulnerabilities
- Implementing security incident response procedures

By following these recommendations, organisations can help secure their IoT devices and protect their data from unauthorised access.

3 IoT applications that should **avoid the public internet _**

A growing number of IoT applications carry sensitive data that businesses cannot afford to expose to the threats of the public internet.

Here we look at 3 use cases that should consider a more security IoT network solution:

1. IoT asset management

Asset tracking makes use of IoT applications to connect items in your company's inventory to your management system, giving you real-time insights such as location, environmental conditions and asset status.

Analysts have identified asset tracking as the fastest growing industrial IoT market and it is expected that most connected devices will be location aware within the next decade. Historically a job for humans armed with clipboards and then spreadsheets, IoT-based asset tracking can significantly reduce human error related to quantities and locations as well as cut down on losses and theft by replacing manual asset management with real-time location systems (RTLS) tracking.

While asset management and supply chain often go hand in hand when it comes to IoT, assets can be much more than product inventory.

In construction or farming, it also includes large, expensive pieces of machinery that are moved from job to job. These require trigger alerts if the equipment is moved unexpectedly, as well as updates on preventative maintenance.
Or asset could refer to your workforce. Outfitted with an on-person tracker, IoT increase safety and whereabouts for workers in remote or dangerous locations, whether the location is indoor or outdoor in large areas such as loggers, forest firefighters, or search and rescue teams and can help you better manage responses to situations from a central command centre.

2. Logistics and supply chain

Adding IoT sensors to shipping containers, crates or trucks gives the asset or inventory a digital footprint, enabling you to track its location and movement in real time.

IoT applications in logistics can help businesses better understand the behaviour of assets. When used in combination with asset intelligence systems, they can help make better decisions, gain real-time operational insights and delivery predictions, opening up new revenue streams.Increasingly, IoT can not only enrich the location and status of a shipping container, but also the cargo inside.

IoT connectivity can relay the status of containers with chilled or frozen functionality, and in cases where shipments of cargo are time sensitive such as with medicine or food, can inform how long the container has been in its current location and if it is expected to reach its destination on time.

For both asset management and logistics, IoT connectivity can help beat inefficiencies in:

- **Container utilisation:** Where are all your containers and are they where they are supposed to be? Are they full or empty? Are the ones with specialist functionality such as temperature control seeing optimal usage?
- **Fleet management:** Supply chain chaos has been in the news a lot recently, as ships trucks and delivery vans face lengthy delays. Sustainability is another core focus for transport companies, which are under more pressure to reduce their carbon footprint.
- Leveraging IoT connectivity, transport companies can track and monitor their fleet in real-time to optimise their fleet, reduce fuel costs and improve overall efficiency.
- **Inventory management:** Historically, inventory management had been a very manual process, largely restricted to endpoints, with an item checked out of location A and logged into location B, and its journey in between these two points remaining 'off radar'.

As a result, assets can and frequently do get 'lost', requiring an employee to spend time tracking them down, or the company writing them off.

An effective end-to-end inventory management setup not only helps with optimisation and rationalisation, but also enables transport and logistics organisations to scale their businesses globally.

3. Payment networks

Payments networks are a vital function of the banking system, enabling frequent touchpoints with customers.

Today point of Sale (PoS) devices take many different shapes and forms – from vending machines, coffee machines and ticket machines – all of which need to be connected directly back to the cloud or data centre, or to a local hub, to relay sales and inventory information.

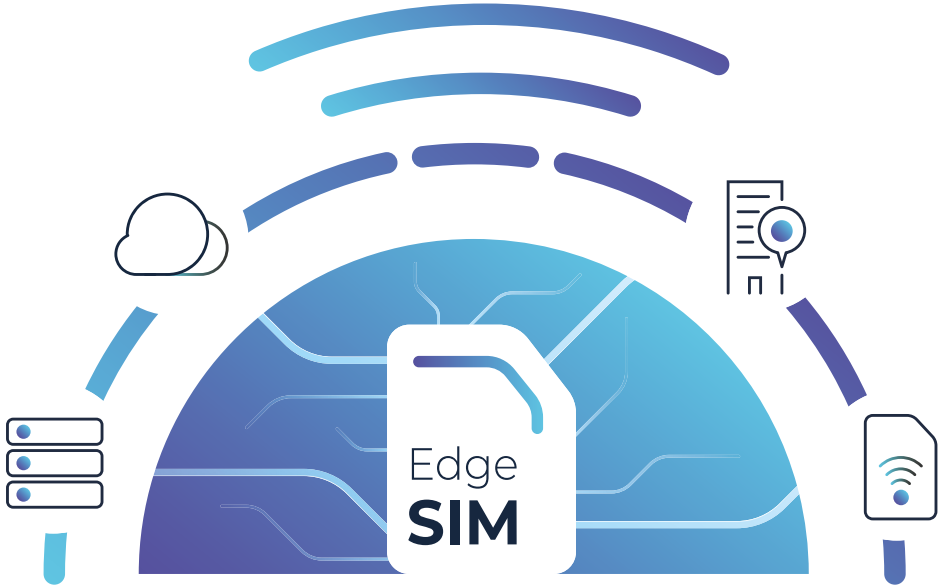
When it comes to payment networks, security is paramount. These networks handle sensitive customer data and transaction information and require a secure path from PoS device to the cloud. There are also data sovereignty and regulatory frameworks to consider.

Introducing **Edge SIM**

Traditional mobile solutions can leave your data exposed to pitfalls of the public internet, while end-to-end private networking solutions, such as VPN, are inflexible and don't offer ubiquitous coverage.

To address this challenge, Console Connect has recently launched **Edge SIM** - the world's first mobile connectivity solution that bypasses the public internet.

Using Edge SIM, businesses can directly connect IoT devices to clouds, data centres, office locations worldwide and manage end-to-end IoT connectivity in real-time through the Console Connect platform.



Book a meeting with one of our IoT experts

How Edge SIM **is different**

Internet backhauling is common practice for most IoT connectivity solutions.

Connected devices are exposed to the public internet when traffic is passed from the mobile operator to back-end applications and hardware.

What makes Edge SIM and Console Connect different is that traffic passes from a mobile gateway directly to a virtual private Layer 3 network, which you can provision and control in real-time. Your traffic completely avoids the public internet.

Why is this important?

	Standard SIM using internet backhaul	Edge SIM using private connectivity
Security	• Insecure and vulnerable to attack • Can expose sensitive data	• Traffic is not exposed to the risks of the public internet • Significantly reduces the threat of a cyberattack
Reliability	• The public internet is best effort • Can lead to service disruption, downtime and loss of business	• The Console Connect network offers an guaranteed level of service • With 99.99% service availability
Performance	• Bandwidth and network speed is not guaranteed • Internet routing is optimised for cost, resulting in inefficient traffic routes	• The Console Connect network offers stringent SLAs, covering jitter, packet loss and latency • Console Connect's private network is optimised for performance and ensures your traffic is delivered via most efficient routes
Best suited for	IoT applications with standard data, including: • Smart home devices & automation • Sensors • Smart wearables • GPS trackers	IoT applications with sensitive or mission critical data, including: • Asset management • Network management • Logistics • Connected cars • Payment networks and POS devices • Live broadcast • Healthcare solutions • Security systems

The most secure way to **access the cloud**

Connect your IoT devices directly to any of the world's largest cloud platforms.

More data is flowing between connected devices and the cloud. As volumes of data grow, take control of your connectivity to the cloud through an automated platform that gives you cloud-like agility and control over your network.

Enabling you to adjust bandwidth to meet the needs of your IoT project.

Manage and pay for both your mobile connectivity and bandwidth-based cloud connectivity through the Console Connect platform - with contracts for as little as a day.

consoleconnect

Find out more

Australia
Level 3 | 200 Mary Street | Brisbane QLD 4000 | Australia

United Kingdom
7/F 63 St. Mary Axe | London EC3A 8AA | UK

France
2/F 16 rue Washington | 75008 Paris | France

Germany
Schillerstr. 31 | 60313 Frankfurt/M. | Germany

Greece
340 Kifisias Avenue/340 Olimpionikon | Neo Psychiko 154 51 | Athens | Greece

United States
475 Springpark Place | Suite 100 | Herndon | VA 20170 | USA

Singapore
6 Temasek Boulevard | #41-04A/05 | Suntec Tower Four | 038986 | Singapore

Hong Kong
20/F, Telecom House | 3 Gloucester Road | Wan Chai | Hong Kong

Japan
11F – 11A-3 | Imperial Hotel Tower | 1-1-1, Uchisaiwaicho, Chiyoda-ku
Tokyo 100-0011 | Japan

South Africa
Building 12 | 1 Woodmead Drive | Woodmead | Johannesburg 2191 | South Africa

UAE, Dubai
Office 401 & 408 | Level 4 | Arjaan Business Tower| Dubai Media City | Dubai

www.consoleconnect.com
Talk to us: sales@consoleconnect.com