IoT Now: ISSN 2397-2793

Q2 2023 • VOLUME 13 • ISSUE 2

# IoT NOW

## HOW TO RUN AN IoT ENABLED BUSINESS

## TALKING HEADS

**Laird Connectivity's Senthooran Ragavan on wireless connections' ability to simplify, streamline and secure industrial operations**

**CONNECTIVITY**
Will new SIMs turn CMPs into springboards? Read the IoT Now report at **www.iot-now.com**

**HEALTHCARE**
Why IoT is improving patient outcomes
See our Analyst Report at **www.iot-now.com**

**UTILITIES**
How IoT is enabling electricity industry transformation
Read the IoT Now Report at **www.iot-now.com**

**IoT SECURITY**
Why enterprises need IoT security-as-a-service
Read the IoT Now report inside this issue

**IoT GLOBAL NETWORK**
Log on at **www.iotglobalnetwork.com** to discover our portal for products, services and insight

**PLUS: 10-page whitepaper** reveals five key factors to consider when building a wireless IIoT system • Complexity and consistency still the main issues find Kaleido's latest IoT connectivity survey • New research reveals radical changes in IoT connectivity management platforms landscape • Why practice makes perfect when it comes to IoT security • Just because the gate's shut doesn't mean it's safe to leave your front door unlocked • Beecham Research shares nine page report on GSMA's new framework for IoT security • The winners of the IoT Global Awards 2023 revealed • News, features and interviews online at **www.iot-now.com**

THALES
Building a future we can all trust

# Thales integrated SIM solutions for IoT

- The certified GSMA Remote SIM Provisioning solution for IoT
- Fully compliant with eSIM services
- The same level of security as eSIM
- Thales-managed security services for streamlined personalization, on-premises or remote

# CONTENTS


## IN THIS ISSUE

# It's not paranoia, they are out to get you

This issue of IoT Now focuses on the challenges associated with securing IoT which seem to have become greater as IoT has matured. This is because of several different stimulae. First, IoT has grown significantly in scale increasing the number of connected devices and with that the threat surface. Second, criminals have had more time to understand IoT, its weaknesses and the transitional spaces and hand-offs which they can exploit. Third, greater understanding has resulted in a substantial reduction in unknown threats with more now identified, the logic dictates there are more threats

The challenge of IoT security is multi-layered, cross-domain and traverses technologies, nations, policies and laws. Therefore, the notion that there's a single genius you can hire to handle security for your company's IoT operations is flawed. The reality is that you'll need a team of geniuses, all skilled in their specific discipline and ready to keep your customers and your devices safe.

That sounds a loud alarm for IoT organisations with business cases based on thin margins. Geniuses aren't cheap to hire and companies that offer services based on the work of geniuses don't sell their services cheaply either. Does this mean IoT security risks have become too great for low margin IoT to mitigate? Are we entering a situation where risk becomes acceptable at various levels of value? Can IoT as a whole be damaged by lack of confidence in its security?

The answer to these questions is, at least partially, yes but IoT will not surrender its potential. Instead, it will find ways to achieve appropriate levels of security. That means not seeking the highest possible level of complete security for a sub-dollar service that doesn't interact with critical systems but making absolutely sure a high-value brand and its customers are protected from life-threatening attacks on critical capabilities as well as from financial damage.

Few enterprises will have the scale and resources to fight the continuous battle for IoT security and this is why IoT security-as-a-service is emerging. It offers the promise that organisations can rely on service providers to secure IoT on their behalf. This brings the benefits of scale to the security fight and enables organisations in various parts of IoT to ensure they can access the appropriate security their use case demands.

**George Malim,** managing editor

IoT can be secured at a sustainable cost in this way, but it demands undiluted focus on using every capability possible to prevent crime. This permeates from the network to the cloud and takes in device identity, network security and software and hardware security mechanisms and that's before we start on security systems and predictive analytics. The next phase of IoT demands not only security tools and rules but also specialists to use them effectively.

Enjoy the magazine!

George Malim

MANAGING EDITOR
George Malim
Tel: +44 (0)7930 301 841
g.malim@wkm-global.com

EDITORIAL DIRECTOR & PUBLISHER
Jeremy Cowan
Tel: +44 (0) 1420 588638
j.cowan@wkm-global.com

DIGITAL SERVICES DIRECTOR
Nathalie Millar
Tel: +44 (0) 1732 808690
n.millar@wkm-global.com

SALES CONSULTANT
Cherisse Jameson
Tel: +44 (0) 1732 807410
c.jameson@wkm-global.com

DESIGN
Jason Appleby
Ark Design
Tel: +44 (0) 1787 881623

PUBLISHED BY
WeKnow Media Ltd. Suite 138,
80 Churchill Square, Kings Hill,
West Malling, Kent ME19 4YU, UK
Tel: +44 (0) 1732 807410

## KORE aims to build IoT hyperscaler with Twilio IoT unit acquisition

**KORE** has agreed to acquire **Twilio**'s IoT business unit as part of its plan to create an IoT hyperscaler. Under the deal, Twilio will receive ten million shares of KORE common stock, which will represent approximately 11.5% of KORE's issued and outstanding shares.

"IoT has immense potential to change the world," said Romil Bahl, the president and chief executive of KORE. "Combining the digital prowess of Twilio's IoT business and the comprehensive connectivity-solutions-analytics portfolio of KORE is a meaningful step toward proliferating IoT and making it more accessible and successful. KORE is thrilled to augment our IoT connectivity as a service (CaaS) offering with Twilio's IoT talent and customer portfolio. This acquisition represents exactly the kind of investment we have said we are willing to make to become an exciting top-line growth company, and specifically, we will benefit from the world-class digital experience and developer community Twilio has built for its IoT business."

This acquisition will bring to market a connectivity suite, including eSIM technologies with KORE OmniSIM and Twilio Super SIM, a one-stop shop for building, deploying, managing, and scaling IoT operations throughout the entire lifecycle via technologies and facilities, and potential for accelerated time to market through global, 24/7

**Romil Bahl, KORE**

customer support and 20 years of IoT experience from the combined operations.

"We are just scratching the surface of the opportunities IoT can unlock for customers," added Twilio's head of IoT, Taylor Wolfe. "As a global leader in IoT, KORE has the right expertise, vision and technology to expand the robust offerings that Twilio's world-class IoT team has built. KORE is the right home for Twilio's IoT business, and we look forward to this acquisition increasing scalability and creating even more powerful business outcomes for our customers."

## Checkpoint Systems on high alert to combat retail crime

**Checkpoint Systems** has acquired Denmark-based **Alert Systems**, an IoT company with a focus on metal and magnet detection in retail environments. Since 1999, Alert Systems has supplied the global retail industry with solutions to identify tools and techniques used by criminals to steal items from stores. These include boosterbags, handmade containers lined with foil used to shoplift, and detachers, illegal magnets used to detach tags with ease. Both are commonly detected at store entrances and exits and in fitting room areas.

Checkpoint has been a partner and distributor for Alert Systems for several years, providing metal and magnet detection products, including Hyperguard, Metalguard and Apparelguard a batch of digital software-driven tools which work against professional shoplifters using boosterbags and detachers to steal items in hypermarkets, fashion stores, pharmacies and other retail stores.

"Organised retail crime (ORC) is increasing globally," said Ben Lilienthal, president of Checkpoint Worldwide. "In the US alone, retailers saw a 26.5% increase in incidents in 2021 and shrinkage represented nearly US$100 billion in losses in 2022. This is due to criminals using increasingly advanced methods of avoiding detection, some of which can defeat traditional anti-theft solutions. By providing retailers with more information regarding when and where ORC threats are entering a store, our new solutions will help retailers drive down the ever-increasing prevalence of gang-related crime."

# News in Brief

## Aeris completes deal for Ericsson IoT Accelerator

**Aeris** has announced the closing of the purchase of **Ericsson**'s IoT Accelerator and Connected Vehicle Cloud businesses and related assets. Ericsson will establish a small stake in the new Aeris. The combination of the merged businesses creates one of the first IoT connectivity management service platforms with operational capabilities worldwide. In combination with its ecosystem of partners across the globe, Aeris will focus on delivering innovative IoT products, services and solutions to enterprises that accelerate digital transformation, drive operational efficiency, and improve customer satisfaction.

Marc Jones, the chairman and CEO of Aeris, said: "We look forward to integrating the Ericsson IoT and Connected Vehicle businesses to create the new Aeris. We have a long history of bringing intelligent innovation to the IoT space and now have additional talent, technology and partnerships to bring that innovation to enterprises looking to simplify, secure and scale IoT around the world."

## 1oT and Workz team up to target US IoT growth

IoT connectivity provider, **1oT**, has partnered with eSIM producer, **Workz**, to serve what it has identified as a gap in the US enterprise market. The partnership guarantees security and rapid implementation of 1oT's M2M global connectivity solutions with Workz's **GSMA**-certified eSIMs and data generation services.

Launched last August, 1oT's remote SIM provisioning platform, eSIM Core, is designed to simplify and reduce the cost of connecting IoT devices for businesses. Certified by the GSMA in October, the system currently manages more than 1.4 million connected devices in 173 countries in sectors such as micromobility, smart cities, autonomous vehicles, agricultural appliances and air monitoring.

## News in Brief

### Colombian taxis tracked with Abeeway

Tunja city, Colombia, has deployed an IoT project to enable tracking of the city's taxi fleet. The system, initiated by **Iluminacion**, a Colombian provider of IoT and renewable energy solutions, is based on **Abeeway** tracking devices and ultra-low power LoRaWAN connectivity for data transfer.

Tunja has a fleet of roughly 1,200 taxis. The drivers are independent and pay for the vehicles with their own money so, if there is aggression towards them or theft of their vehicle they incur financial loss and have no protection. The city approached illuminacion, which led to an initial ongoing pilot project to the first batch of 200 taxis across the city. The city has already approved the deployment of 1,000 more tracked taxis. The project is based on Abeeway Micro Trackers that are connected to the 12V socket of the car for constant power supply and provide location information every three minutes throughout the day.

### ACA Pacific and Atsign partner to deliver IoT security

**ACA Pacific Singapore,** an IT marketing and value-added distributor in the Asia-Pacific region, has partnered with **Atsign**, a provider of IoT security, to bring IoT device security technology to the region. The adoption of IoT devices has led to an increase in criminal hacking groups attacking these devices to gain access to various organisations, as well as the government's critical infrastructure.

ACA Pacific Group will offer Atsign's technology platform to eliminate all network attack surfaces which will thwart cybercriminals, protect IoT devices and save costs over traditional, complicated, and less secure means of protecting IoT devices. Atsign will work closely alongside ACA Pacific's broad ecosystem of partners to deliver cybersecurity solutions across industries and use cases.

### e& and E-Space to develop IoT and digital transformation offerings

**e&**, formerly known as Etisalat Group, and **E-Space**, a global space company focused on bridging earth and space with sustainable low earth orbit (LEO) networks, have announced plans to develop advanced global IoT, smart IoT and digital transformation offerings. The collaboration seeks to maximise the end user value derived from borderless smart connectivity and digital capabilities across land, sea and sky applications.

The co-operation will focus on the creative development of cloud-native digital and IoT solutions optimised with edge-based artificial intelligence (AI). By using e&'s terrestrial infrastructure and E-Space's space system, including its global LEO constellation and unique device capabilities, the two organisations will create new business models to elevate IoT and digital transformation agendas of governments and large-scale enterprises worldwide.

Mikhail Gerchuk, the chief executive officer of e& international, said: "Telecommunications and space

**Mikhail Gerchuk, e&**

technology have a natural synergy, offering enormous opportunities for telco companies to expand their reach and capabilities. With our advanced infrastructure and E-Space's next-generation space system, optimised with edge AI, we will offer a multi-technology platform enabling our customers to embrace a digital-first lifestyle more efficiently. We are confident that we can use our combined expertise to create global digital IoT experiences to help our customers advance their digital transformation plans."

### BAI rebrands as Boldyn and scores NYC MTA network expansion

**Transit Wireless**, a **BAI Communications** company and 5G wireless infrastructure provider, has announced a network expansion partnership with New York City's **Metropolitan Transportation Authority** (MTA) which will double the size of Transit Wireless' 5G fibre network including 418 track miles and up to 20 separate river crossings. The neutral host provider will expand its high-capacity fibre connectivity designed and built for carrier-grade 5G cellular service, small cell deployment, offload and roaming services, and network edge colocation. The network will be designed to support more than ten million users per day and allow mobile network operators to offer their customers enhanced data and voice service underground and throughout the entire NYC subway.

The rebrand to **Boldyn Networks** will bring together BAI's six operating companies and BAI will begin operating officially as Boldyn Networks at the end of June 2023. Established in Australia in 1923, BAI has a 100-year pedigree in broadcast and telecoms solutions. In the last two years, BAI has grown by acquiring **Mobilitie**, **Signal Point Systems** and **ZenFi Networks** in the United States, and **Vilicom** in Ireland and the UK. It also secured multi-year agreements to deliver connectivity services on transport networks in London and New York; was awarded a 20-year

**Igor Leprince, Boldyn Networks**

partnership with **Sunderland City Council** to create the UK's most advanced smart city; and expanded into Italy, its first operation in mainland Europe. All companies, in addition to Transit Wireless, which has been part of the group since 2010, will become one team and adopt the Boldyn Networks brand.

"By launching Boldyn Networks we're bringing together the power of all our businesses under one brand and creating the global neutral host partner of choice for customers," said Igor Leprince, the group chief executive of BAI Communications. "We will be integrating a portfolio of neutral host solutions, supported by a team of diverse and highly skilled experts, and years of experience in the public and private sectors."

## Amazon invites developers to test Sidewalk and build apps with new tools and resources

**Amazon** has announced that Amazon Sidewalk, a secure, low-bandwidth, long-range network that utilises Bluetooth Low Energy and other low power wide area (LPWA) connectivity to enable devices to connect to a series of mini-mesh networks enabled by its Ring cameras and Echo speakers, is now open for developer testing. Sidewalk coverage now extends to 90% of the US population, the firm says, and free test kits are available for developers to validate Sidewalk coverage for themselves as they build Sidewalk devices.

"We've rapidly built out a long-range, low-bandwidth network and this is an open invitation for developers to put it to the test," said Dave Limp, the senior vice president of Amazon devices and services. "Many types of connected devices have been limited by the range of Wi-Fi and the cost of cellular technology, which has hindered the ability to connect devices like environmental sensors, leak detectors and smart locks. Sidewalk is designed to provide a secure, low-cost way to invent and connect a whole new range of devices, and we can't wait to see what developers build."

Devices connected to Sidewalk come with a secure, persistent and low-cost connection to the cloud. Newly-released maps detail estimated Sidewalk coverage for any US location, enabling developers to understand if their devices will connect in a desired area before starting product development. Sidewalk test kits are designed to validate real world coverage by regularly pinging their location over the network, providing clear signal strength readings on a map within a developer portal.

**Dave Limp, Amazon**

"The integration of AWS IoT Core and Amazon Sidewalk marks a significant milestone for developers, manufacturers and customers, streamlining the design, connection, and deployment of Amazon Sidewalk based IoT solutions," added Yasser Alsaied, the vice president of IoT at Amazon Web Services. "Now, with AWS IoT Core for Amazon Sidewalk, developers can access more than 200 AWS services to build scalable solutions on top of a highly reliable, secure and free-to-connect wireless network."

## Shipments of smart home devices set to bounce back in 2023, says IDC

Global shipments of smart home devices declined for the first time in 2022 as shipments fell 2.6% year over year to 871.8 million units, according to the **International Data Corporation** (IDC) Worldwide Quarterly Smart Home Device Tracker.

Smart TVs, which represented the largest category, experienced a 4.3% decline in 2022 due to tough year-on-year comparisons as the market for TVs and other products was extremely strong in 2021 due to Covid-related purchasing. Looking ahead, IDC forecasts a modest 2.2% growth in smart home device shipments in 2023 as the global economy recovers. This growth is expected to continue through 2027 with device volumes reaching 1.23 billion in 2027.

"Smart TVs will likely face another year of decline in 2023 due to macroeconomic pressures and long replacement cycles," said Jitesh Ubrani, research manager for IDC's Mobility and Consumer Device Trackers. "With the recent entrance of value-oriented brands such as **Amazon** and **Roku**, IDC expects further declines in average selling prices for TVs while also bringing premium features down to more affordable price points."

Apart from TVs, most other smart home categories such as security cameras, connected doorbells and door locks along with smart displays are expected to grow thanks to a developing installed base, a recovering economy, and the rise of emerging markets.

# News in Brief

## L-com adds to range of IoT light sensors

**L-com**, an **Infinite Electronics** brand and a supplier of wired and wireless connectivity products, recently announced the expansion of its line of IoT light detection environmental sensors. The sensors gauge either ambient or ultraviolet light.

The new sensors assist in the use of IoT data collection to make process control more efficient and to lower building and process costs. Applications for the light-detection sensors include greenhouses, agriculture, solar farms, labs, factory floors, manufacturing and general environmental monitoring. The wall-mount ambient light models measure light intensity up to either 65,000 Lux or 200,000 Lux. They have a waterproof housing and are suitable for outdoors as well as demanding indoor environments such as factory floors.

## Soracom adds industrial SIM to IoT SIM portfolio

**Soracom** has added an industrial grade SIM card to its portfolio of IoT SIM and embedded SIM (eSIM) solutions. With this addition, Soracom now offers both standard and industrial-grade eSIMs and SIM cards, as well as integrated SIM (iSIM) capability.

The Soracom industrial SIM card is designed for M2M/IoT applications where environmental conditions demand a rugged solution and a card-type SIM is preferred to an eSIM. The industrial SIM supports mini, micro or nano form factors (2FF, 3FF or 4FF) and offers a coating as well as enhanced chip characteristics to limit erosion and resist extremes of temperature, humidity and vibration.

# Industrial organisations turn to wireless connections to simplify, secure and streamline operations

As Industrial IoT (IIoT) gathers momentum and connection numbers hit hyperscale volumes, wireless connections are offering a compelling blend of flexibility, performance and cost efficiency. Options extend from low-power technologies such as Bluetooth Low Energy (LE) and LoRaWAN to the latest high-performance variants of Wi-Fi and cellular technologies. These technologies introduce a reality of no cables and the benefits of mobile, battery-powered equipment to industrial environments. However, in addition to these benefits, industrial organisations need to have complete trust in the security and reliability of device connections and have confidence that devices will be simple to deploy, configure and maintain. Senthooran Ragavan, a senior product manager at Laird Connectivity, tells IoT Now managing editor George Malim how industrial organisations' appetite for wireless connections is maturing and details how IIoT is being aided by a world of wire-free possibilities

***As always, cost-efficiency is the bottom line, and industrial organisations want wireless solutions that provide good value for money***

**George Malim: Industrial environments are increasingly turning to wireless technology to benefit from the flexibility and performance that wireless equipment can now support. What are industrial organisations' priorities when they select wireless connectivity?**

**Senthooran Ragavan:** There are many. For one, it makes establishing predictive maintenance models much easier. Keeping machines running is critical, and when they fail, it's very costly. One example: Siemens found last year that downtime in an auto plant costs on average US$2 million per hour. Wirelessly monitoring and analysing machinery for signs that it needs maintenance – and doing that maintenance exactly when it's needed – is a tremendous advantage for industrial operations. Doing this wirelessly makes connecting an entire site much easier – no miles of wires, no cables, just reliable up-to-date data.

A further challenge is scalability. Industrial organisations require wireless solutions that can be easily scaled up or down to meet changing business needs. It is very easy with wireless solutions to add or remove additional devices without compromising their existing setup. Device management solutions such as our Canvas Device Manager help organisations to easily manage devices remotely and scale without disruption.

Another priority is interoperability. Industrial machines are often complex systems with a mix of wired and wireless components. Wireless solutions such as our BT610 I/O Sensor are designed for industrial equipment with several flexible interfaces in mind. The BT610 takes in data from multiple types of inputs and sends it reliably over Bluetooth LE, creating a kind of common language among many different kinds of machines in a single facility.

As always, cost-efficiency is the bottom line, and industrial organisations want wireless solutions that provide good value for money, balancing the cost of deployment and maintenance with the benefits gained from increased flexibility and performance.

Finally, ease of deployment and management is an essential requirement. Wireless technology should be easy to deploy and manage, allowing for quick installation and efficient maintenance without the logistics of cabling and wiring. Sometimes it's impossible to install a wired sensor. Sometimes the machine in question is mobile – it cannot be tethered. Wireless creates opportunities that might not otherwise exist with minimal power consumption and reliable connection. Organisations want solutions that are simple to configure and troubleshoot, reduce downtime and ▶

**SPONSORED INTERVIEW**

***Adoption of wireless solutions for machine monitoring has increased significantly***

**Senthooran Ragavan**
**Laird Connectivity**


**Laird Connectivity**
**BT 510**

increase productivity. Wireless sensor devices, telemetry platforms, and device management platforms hit that target.

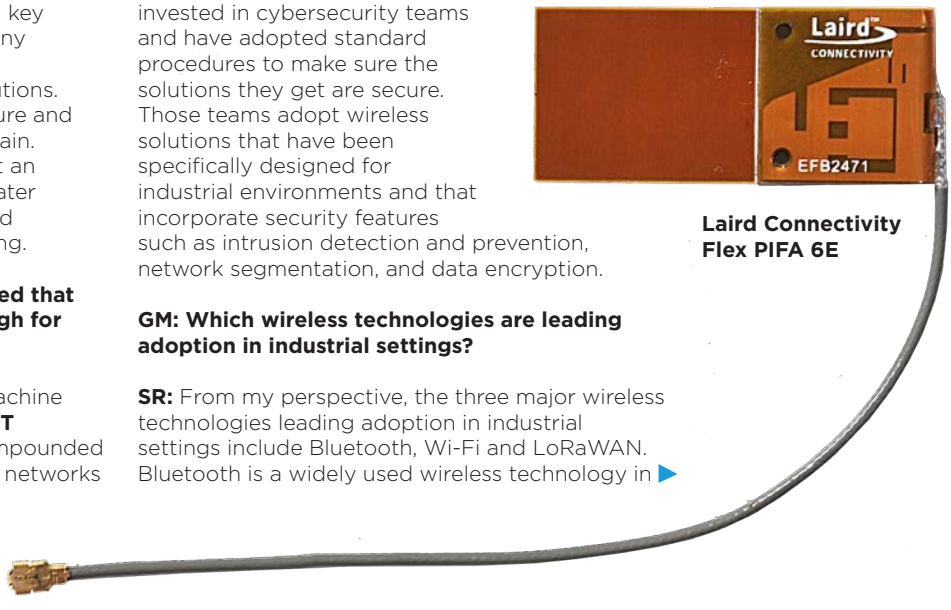
**GM: There are obvious advantages to removing cables from factories. They are expensive to re-route, can be trip hazards, can be damaged easily, and are expensive to replace at upgrade time. Is this the key driver for organisations going wireless?**

**SR:** These are certainly some of the main key drivers, but the major driver is that in many industrial environments it is very hard or impossible to physically install wired solutions. These require very high capital expenditure and demand a lot of time to install and maintain. Again, for mobile machinery, cabling isn't an option at all. Wireless solutions offer greater flexibility, enabling ease of installation and maintenance. That makes them compelling.

**GM: Are industrial organisations satisfied that wireless is now secure and robust enough for their use cases?**

**SR:** Adoption of wireless solutions for machine monitoring has increased significantly. **IoT Analytics** estimated in 2022 that the compounded annual growth rate of WPAN and WLAN networks for the IoT would rise 22 to 24% between 2021 and 2025. However, there are still some legacy concerns about the security and robustness of wireless technology in industrial environments. Wireless technology has dramatically evolved (WPA3 for Wi-Fi 6/6E, LE Secure Connections for Bluetooth LE, and more) and many industrial organisations are now increasingly satisfied that it is secure and robust enough for their use cases.

Organisations commonly have invested in cybersecurity teams and have adopted standard procedures to make sure the solutions they get are secure. Those teams adopt wireless solutions that have been specifically designed for industrial environments and that incorporate security features such as intrusion detection and prevention, network segmentation, and data encryption.




**Laird Connectivity**
**Flex PIFA 6E**

**GM: Which wireless technologies are leading adoption in industrial settings?**

**SR:** From my perspective, the three major wireless technologies leading adoption in industrial settings include Bluetooth, Wi-Fi and LoRaWAN. Bluetooth is a widely used wireless technology in ▶


**Laird Connectivity Sentrius BT610**


**Laird Connectvity Sentrius MG100**


**Laird Connectivity BL340PA**

***LoRaWAN is an ultra-long-range, low-power wireless technology that is widely used for IIoT applications, particularly for remote monitoring and control***

industrial settings, particularly for low-power applications such as sensors, wearables and other IoT devices. Bluetooth offers low power consumption, short-range communication and easy pairing, making it ideal for many industrial applications. Bluetooth has evolved from classic Bluetooth to Bluetooth 5.4, which includes the low energy feature (LE) coded PHY. This increases the transmission range of the technology at the cost of lower data rate. It's popular in harsh RF environments like industrial, where lots of signal and reflective surfaces require wireless solutions to cut through the noise. This low power consumption results in technology being used in battery-powered sensor devices. **Laird Connectivity** has a comprehensive range of Bluetooth modules that targets industrial devices and gateways and enables customers to easily collect and send data to cloud servers.

Wi-Fi is one of the most widely adopted wireless technologies in industrial settings due to its widespread availability, high bandwidth and low latency. Wi-Fi is actually so ubiquitous that industrial facilities may already have access points in place, lowering the barriers to entry. Wi-Fi can be used for a wide range of industrial applications, including machine-to-machine (M2M) communication, inventory management and remote monitoring. Enterprise-grade Wi-Fi service provides exceptional performance, security, standards/compliance and lifecycle management – factors that are important for connectivity in any IIoT system. Wi-Fi 6 and 6E also support some of the most current security offerings, such as WPA3. Laird Connectivity offers industrial-grade Wi-Fi modules and robust IoT gateways to enable customers to develop devices for industrial environments.

LoRaWAN is an ultra-long-range, low-power wireless technology that is widely used for IIoT applications, particularly for remote monitoring and control. The robustness of the protocol enables devices to operate seamlessly in the harshest environments where other technologies struggle to send data. The ability to transmit very long distances (up to 10 - 15 km) and the ability to run LoRaWAN devices on a battery for a longer period make it a very attractive technology for IIoT applications.

LoRaWAN operating in the Sub GHz ISM band (863-870MHz / 902-928MHz) allows greater range and better propagation through various building materials compared to Wi-Fi or Bluetooth LE. The data transmitted over LoRaWAN is end-to-end encrypted, making communications secure and protected from unauthorised access. Laird Connectivity offers LoRaWAN modules, sensors and gateways that enable customers to easily collect and send sensor data over LoRaWAN.

**GM: What is Laird Connectivity's approach to this market? How do you prioritise device design for industrial organisations?**

**SR:** Laird Connectivity tries to address each element that has been explained above by providing both modules and finished IIoT devices for the industrial environment. ▶


**Laird Connectivity**
**Sterling LWB5+**


**Laird Connectivity**
**RG1xx LoRa Gateway**

Our portfolio is particularly reliable and durable. Our modules and devices are purpose-built for industrial environments; at minimum they support the industrial temperature range of -40 to +85°C. Some support even more, up to +105°C for more extreme use cases. IoT devices are designed using durable enclosure material with IP ratings ranging from IP65 and IP67.

Security is critical for us in the industrial space, and we take ensuring secure data transfer between devices very seriously. Particularly in Wi-Fi, we provide the **Summit Suite**, a full enterprise-grade security architecture that goes well beyond stock security offerings for these critical devices. It includes:

- **Secure connectivity** - Enhanced regulatory support, WPA2-Enterprise, WPA3-Enterprise and TLS 1.3.
- **FIPS cryptographic modules** - FIPS 140-2 Level 1 validated, with a roadmap to validate to FIPS 140-3 Level 1. Secure data-in-transit and data-at-rest.
- **Chain of Trust device security** – Secure enclave and validated software images from the bootloader down to user applications with device encryption and secure key storage.
- **CVE monitoring and remediation** – Detects, vulnerabilities in the software packages your devices use with regular scans and updates.

For IoT devices, our Canvas Device Manager, powered by **EdgeIQ**, simplifies workflows for configuration and maintenance of your IoT device deployments. This allows you to easily set up devices, monitor status and keep software up-to-date across your entire IoT device fleet, particularly important for organizsations with a high number of devices that may be very far apart.

We also provide long-term support for hardware and software products and providing simple and easy upgrade paths. This means that the customer will not have to worry about redesigning their hardware or solution. Our Summit SOM 8M Plus is designed with 10+ year life cycles in mind.

**GM: How do you see the future of wireless connectivity in industrial environments?**

**SR:** LoRaWAN and Bluetooth are commonly used and will be the most used sensor communication protocols due to the advantages they have in their own capabilities. Bluetooth is going to lead in the market for sensors that are targeted at personal area network (PAN) applications. LoRaWAN on the other hand will see great growth compared to other LPWAN technologies such as narrowband IoT (NB-IoT) and LTE-M. NB-IoT, although strong, has much more focused success and massive growth in China where LoRaWAN lags behind.

There will be much more emphasis on security of devices and more organisations will start to adopt device management platform solutions to manage their ever-increasing sensor deployment. Upcoming technologies such as Wi-Fi 6E, ultra-wideband (UWB), private 5G networks, and Wi-Fi HaLow are some of the new technologies to look out for in the industrial space.

***Security is critical for us in the industrial space, and we take ensuring secure data transfer between devices very seriously***

**www.lairdconnect.com**

# How to make wireless IIoT work for your business

Laird™
CONNECTIVITY

# Five factors to consider if you're building a wireless IIoT solution

IoT, or the Internet of Things, means a lot of things to a lot of people. At its core, it's about connecting the real world of products and environments to the internet where that data can be used to help improve life. Unfortunately, that's a really broad description. It's how we end up with the endless list of IoT niches we see today: smart cities, smart buildings, industrial Internet of Things (IIoT), M2M, consumer IoT, eHealth and many more

To cut through a lot of confusion and help you decide if you want to read this whitepaper, ask yourself three questions:

1. Do you belong to an enterprise looking to create revenue from your customer base through a connected solution?
2. Do you consider your business to be mission-critical? That could mean many things, but some examples could be helping your customers meet regulatory compliance, preventing downtime of expensive assets, or protecting the health and wellbeing of patients. It does not include helping your customers perfectly toast bread at precisely 6:45am each day.
3. Are you looking for help on selecting the right sensing and connectivity technologies for your IoT architecture?

If you answered yes to one or all of the above – great! We think you'll get something out of this white paper. Let's get started.

This whitepaper examines the benefits as well as the complex challenges that accompany the implementation of an enterprise-grade, revenue generating IoT solution. Navigating the system complexity, creating the appropriate connectivity architecture, managing effective security, are some of the challenges that must be addressed and solved for an effective, profitable and scalable system. This paper highlights the following five factors to consider when building an IIoT solution:

1. Top IoT challenges
2. What your competitors are doing – example applications
3. Architecting your IoT solution
4. Choosing a connectivity option
5. Selecting a cloud solution

For the sake of simplicity, we'll call you an original equipment manufacturer (OEM) in this whitepaper. That could mean you actually manufacture equipment such as medical devices, industrial pumps or devices in commercial restrooms. Or it could mean you develop a software solution that uses data from other companies' equipment and sensors to drive insights for customers. ▶

This whitepaper examines the benefits as well as the complex challenges that accompany the implementation of an enterprise-grade, revenue generating IoT solution.

## The importance of connected products to OEMs

OEMs are increasingly under pressure to build their business – outperform competition, increase revenue and grow profit margins. When manufacturers are looking to improve their business or systems, when they're seeking to drive business growth, they typically don't go out searching specifically for an IoT or connected system. What these business drivers are seeking is simply a way to increase the size and profitability of their business. They are looking for a solution that will meet their business outcome goals.

Although it's true that an IoT system and the data that results from it can vastly transform a business, most manufacturers are looking for ways to achieve one or more of the following:

- Help your customers have the best possible experience and uptime with your products
- Help your customers reduce their own costs by automating a previously manual solution (We're looking at you, Mr. Clipboard)
- Help your engineers and product managers understand how your customers use your products
- Help your field service teams be more efficient and profitable

To put it simply, IoT just isn't that interesting unless there is a solid business case surrounding it; an obvious reason to build a connected system. It's important to emphasise to potential customers how an IoT system can help them make great strides towards achieving their business goals.

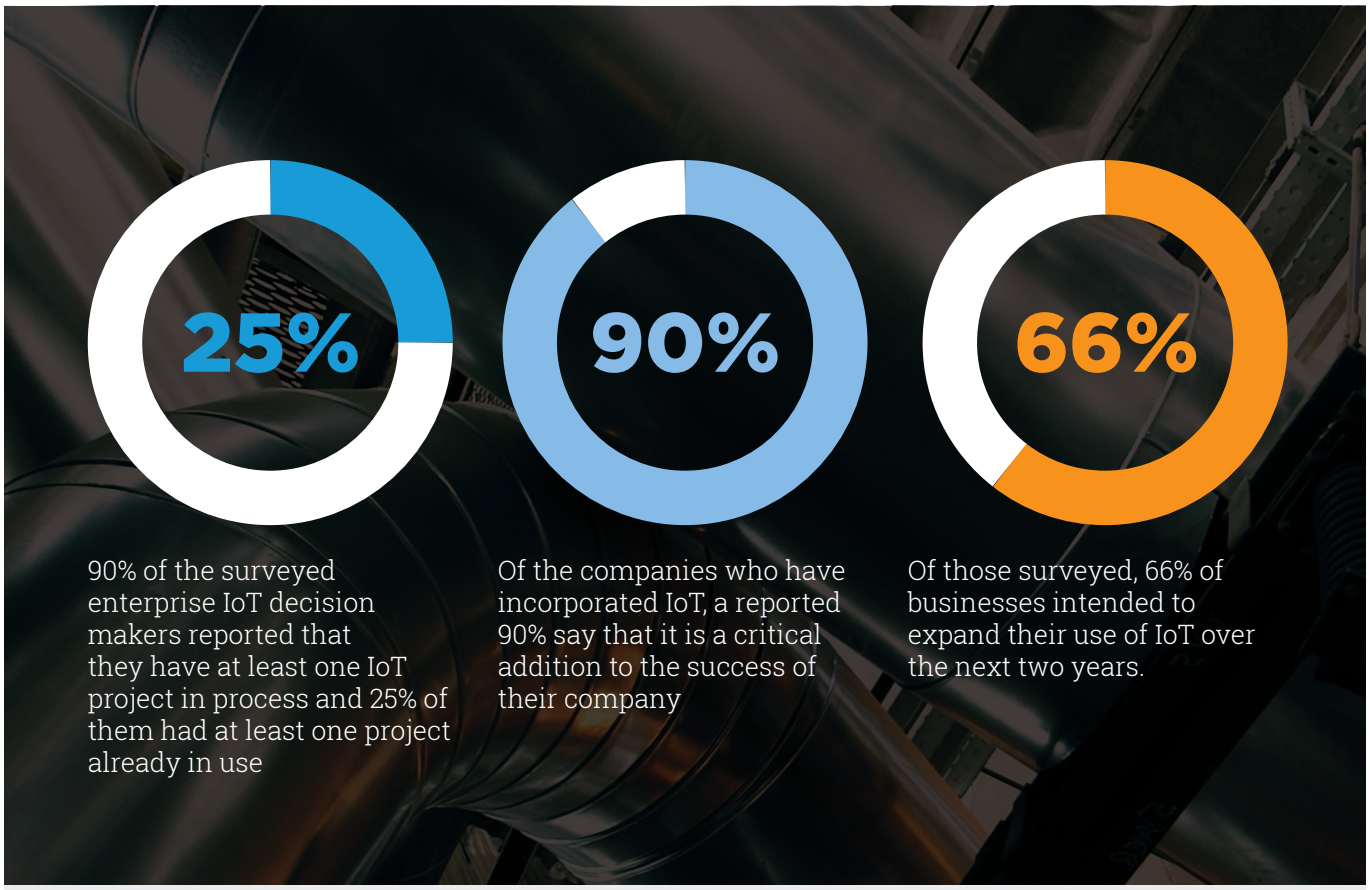
But if you're reading this whitepaper, it's probably a safe bet that you've already figured this one out. Your job now is to make that business case a reality, preferably stumbling as few times as possible along the way.

## Top IoT challenges

Connected solutions can generate a lot of useful insights, but in between your things, the internet, and the insights you seek are infinite combinations of specialised technologies: wireless, sensors, operating systems, cloud, containers, security, SaaS systems, analytics engines and user interfaces. Piecing these technologies together into a value-driver is fraught with challenges, including:

- Picking winning technologies in your solution that will stand the test of time
- Assessing and maintaining return on investment (ROI) for both upfront development as well as ongoing costs of maintenance
- Integrating legacy products and systems
- Finding the diverse skill sets necessary for successful IoT implementation
- Ensuring that your IoT system is secure

In spite of this, adoption of IoT across industries continues to increase at a fast pace. According to the most recent **IoT Signals** survey completed by **Microsoft**, 82% of the surveyed enterprise IoT decision makers reported that they have at least one IoT project in use. Of the companies that have incorporated IoT, a reported 90% say that it is a critical addition to the success of their company, with a 96% reported satisfaction rate with the results. ▶




It's evident that the move towards IoT systems continues to grow. Also, according to the Microsoft survey, 90% of businesses were already IoT adopters with 66% planning on expanding their IoT implementations over the next two years. As these businesses experience an increased ROI, they are also likely to continue to look for new ways to use this IoT technology, especially as additional innovations such as artificial intelligence (AI) and 5G emerge.

Simply put, companies that successfully deploy connected solutions to the benefit of their business will thrive, and those that don't will fall behind. 90% of the surveyed enterprise IoT decision makers reported that they have at least one IoT project in process and 25% of them had at least one project already in use. Of the companies who have incorporated IoT, a reported 90% say that it is a critical addition to the success of their company. Of those surveyed, 66% of businesses intended to expand their use of IoT over the next two years.

## Prerequisites

There are a few important decisions you'll need to make that are out of the scope of this whitepaper. Before selecting an IoT architecture, it's vitally important that your organisation is aligned on where you stand on the following:

- How do you plan to monetise your IoT solution? As previously discussed, will you be helping your customers? Engineering team? Field service organisation?
- What equipment or environmental data (temperature, vibration, usage or current) do you need to drive the insights you desire. This expertise likely already lives in your organisation. If you don't know, that's OK – but you should be ready to cast a wider net and give yourself a longer leash on a proof of concept phase to learn what's necessary to gather and what isn't.
- Your organisation's long-term IoT strategy – where do you plan to invest your resources and gain an edge? Do you need machine learning experts? Full stack developers? Big data analysts? This whitepaper assumes, as we see with many of our customers, that the data you gather, the algorithms you develop, and the cloud systems you intend to build are going to be your company's secret sauce for IoT.
- Where is the data you need? Is it already living in unconnected legacy equipment? Does it need a new sensing capability?
- What's going to collect that data? Do you need to install new equipment? Retrofit legacy products? Can your customers install this equipment or do you need to send out installers to your customer sites?
- In what type of environment is your equipment and how will it get out? Will you have Wi-Fi access? Cellular reception?

Understanding these basic realities will help guide which architectures and technologies might be a good fit.

## Example applications

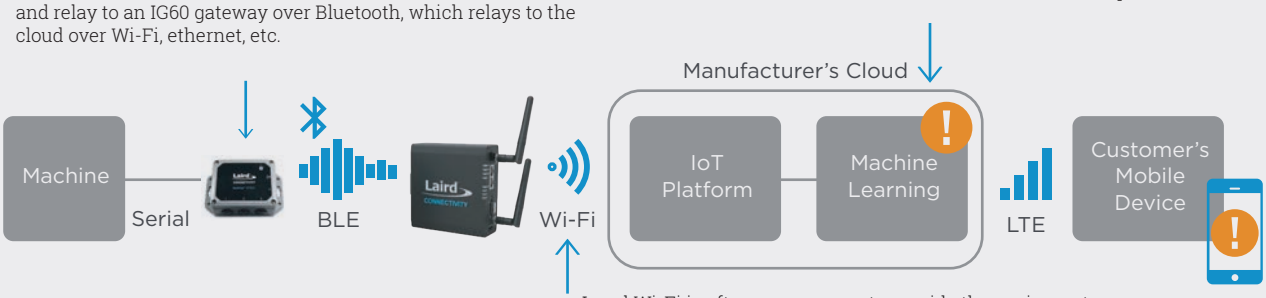
To get you started down the right path, below are some examples we've seen: ▶

## *Smart industrial support systems*

### Solution architecture

Legacy equipment frequently uses RS-232 (serial) based-protocols. A BT610 sensor can extract useful data over wired serial connection and relay to an IG60 gateway over Bluetooth, which relays to the cloud over Wi-Fi, ethernet, etc.

Machine learning algorithms in the cloud can predict failures and warn customers with alerts to their smartphone




Local Wi-Fi is often an easy way to provide the equipment secure connectivity to the manufacturer's cloud environment

Several customers we work with design and manufacture equipment that keeps mission critical systems running. For example, it could be a cooling system that's keeping a semiconductor laser etcher running, a compressor system keeping lubricant running through a fabrication machine, or a backup power system connected to hospital refrigerators.

In any of these scenarios, these manufacturers put their companies and brands on the line to guarantee reliability and uptime. When their equipment fails, it causes other major systems to fail, causing their customers to lose thousands of dollars an hour from lost production.

For this class of company, a connected solution offers several paths to monetisation:

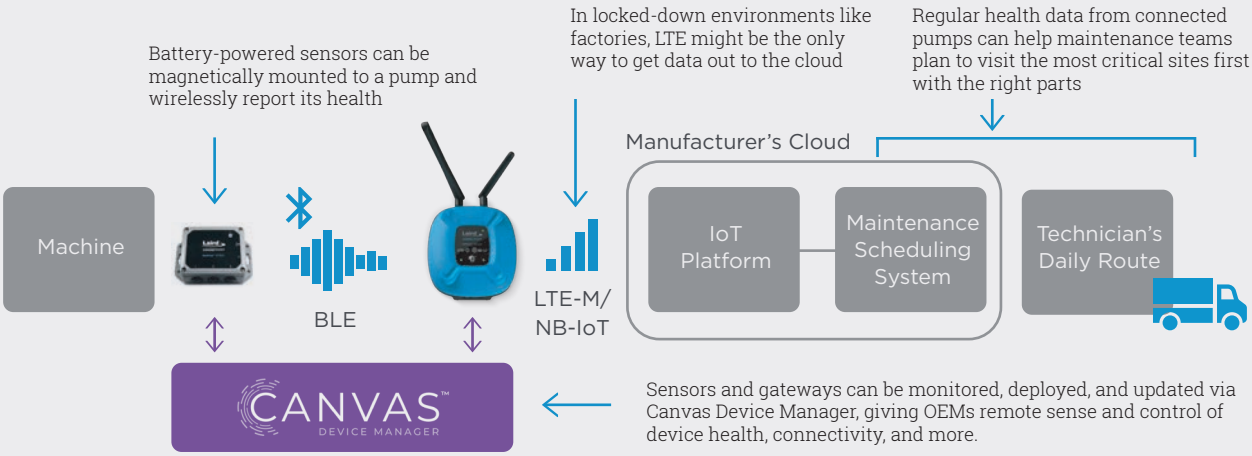
Offer higher levels of service level agreements (SLAs) to their customers from the ability to monitor equipment in the field and predict failures through a connected solution.

Increase revenue from aftermarket parts or consumables by ensuring customers properly maintain the equipment.

Reduce field services teams' costs by allowing them to optimise routes and service the most urgent issues first. ▶

## *Connected pumps and compressors*

### Solution architecture




Some technologies and inventions are high-end and trendy. Others are a less glamorous but no less important. For example, consider pumps and compressors. We have customers whose main priority or function is to provide equipment that pumps drinking water to both urban and rural areas as well as to treat and remove wastewater.

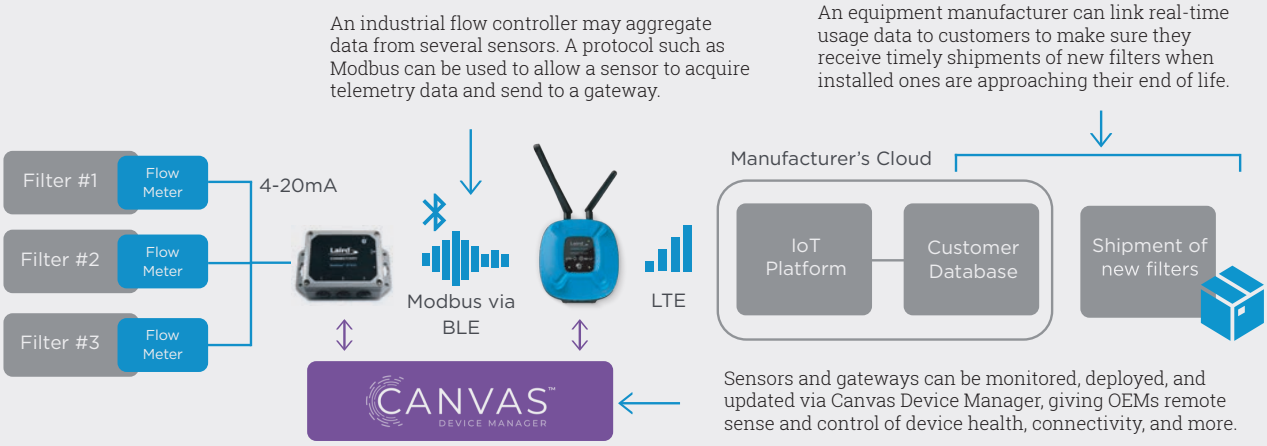
Not a fancy technology but it certainly plays a critical, life-saving role. If critical installations such as wastewater pumping stations, water treatment plants, and irrigation systems fail, it not only creates increased mechanical expense and the expense involved with business down-time, it threatens life and livelihood of those who rely on the services the equipment provides.

For this type of company, a connected solution offers the following possibilities for enhanced business opportunities:

Provide cost savings to their customers by enabling remote monitoring of in-service equipment. With this ability to remotely monitor equipment, customers are able to perform predictive maintenance techniques rather than routine preventative maintenance – equipment is only serviced when necessary rather than on a time-based schedule. This decreases the number of unexpected mechanical failures, prevents unnecessary equipment down-time, and minimises the need for personnel to manually inspect critical installations.

Increase revenue by providing a system for their customers to receive operational data that can enhance or guide business goals. ▶

## *Filtration systems*
### Solution architecture



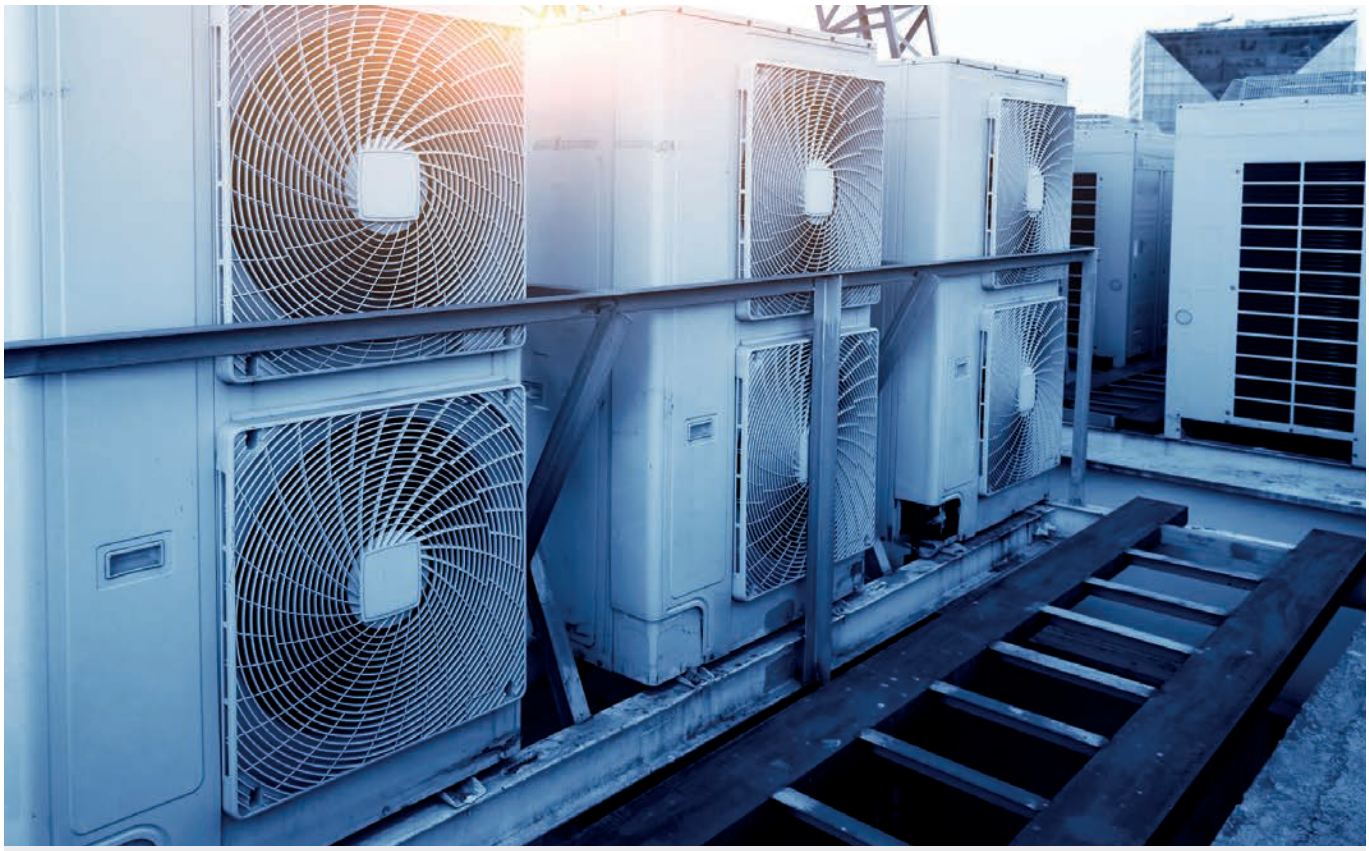

Probably a less life-critical example but still a solid application of a connected solution can be seen in the beer-brewing industry. Considering the increasing amount of beer competition and knowing that beer drinkers are often very particular about their beer selection, breweries strive for high quality and consistency in their brewing process. Companies that provide filtration systems to these breweries could benefit from the business opportunities a connected solution provides.

There are multiple ways that a connected system could enhance a company's offerings or services and therefore their financial bottom line.

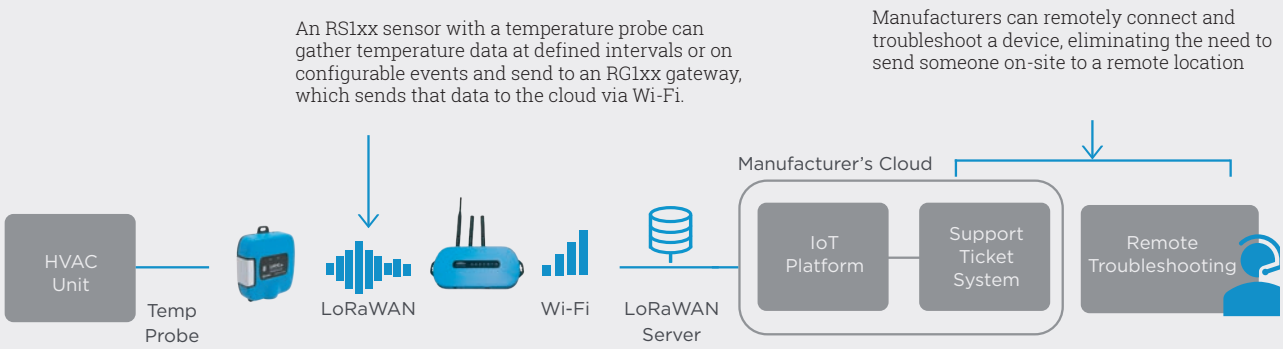
In addition to previous examples such as enabling predictive maintenance and decreasing field service team costs, the following are also possible with a connected solution in the brewing industry:

Provide their customers the ability to easily monitor the entire brewing process to ensure production consistency and quality. The ingredients that go into beer can vary from year to year depending on environment conditions, such as weather and soil. From the data provided by a connected IoT system, brewers can make the necessary adjustments to ensure each batch of beer tastes as it should.

Create a connected system for their customers that operates in a secure environment and ensures no loss of data even when Wi-Fi connectivity is not available. ▶



## *HVAC monitoring*
### Solution architecture




Downtime in any manufacturing plant is a threat to the business. As the old saying goes, "time is money". When a plant is idle, for whatever reason, it's a financial risk to the business. A connected IoT solution could enhance business success for any type of manufacturing plant where asset management, operational efficiencies, and safety are critical factors. Take, for example, a company that provides gear drives to manufacturing plants.

For this type of industry, offering smart gear drives as part of a connected system could enhance business opportunities in a variety of ways:

Offer real-time monitoring of equipment to ensure optimal performance and maintenance needs.

Provide on-demand information to customers.

To ensure efficient product installation as well as historical and analytical data to assess equipment performance.

Enable predictive equipment analysis to not only allow timely maintenance but to also ensure a safer work environment for employees. ▶

### Connect to legacy sensors
Analogue and/or digital IO sensors that already exist in your system communicate data to a wired communication bus sensor via a modbus. The sensor then delivers the data to a gateway, which communicates with the cloud.

### Connect to wireless sensors (battery-powered)
Battery-powered Bluetooth or LoRa sensors communicate wirelessly to a wired communication bus which then delivers data to and from the cloud.

### Direct integration
Your machine or device contains an integrated module or modem to directly communicate to and deliver data to and from the cloud. An example module is the Laird Connectivity Pinnacle 100 multi-wireless modem.


# *Architecting your IoT solution*
## Choosing connectivity options

With an IoT connected system, data is mission critical. Most of the value to your business comes from the resulting data once it's transitioned to the cloud. To complicate this issue, industrial buildings and factories frequently have harsh radiofrequency (RF) environments and are, at times, in remote locations with poor carrier coverage.

But, how exactly do you get this data? How is this data effectively moved to the cloud? The first step is to determine which connectivity options are available to you. Here are some things to consider:

- What connectivity options are available at your site? Will the local IT allow you to access and use the Wi-Fi network? If not, are you able to run Ethernet cable?
- Are there currently sensors available to use with the system or will you need to install new ones? How will you power the sensors? Are they battery-operated?
- Is a wireless connection an option for the sensors based upon the environment? Is the environment conducive to the use of sensors?

With an abundance of technologies available at your fingertips such as Bluetooth, Wi-Fi, LoRa and cellular, along with cloud systems to collect, store and analyse data, where do you start? How do you even begin to choose the correct connectivity choice for your industrial IoT systems and applications?

### Connectivity architectures
As shown in the previous examples, there are many ways to move the data you need for your connected solution to the cloud. Here are some generic examples to consider.

### Selecting a wireless technology
There are four main wireless technologies that should be considered for connectivity in a wirelessly connected system: Wi-Fi, Bluetooth, cellular and LPWAN. Connectivity can be embedded within the device or added on with external modules and devices once the device has been deployed. Market expectations are that new smart devices have connectivity embedded within the device, but many businesses still utilise legacy devices which must be taken into consideration. Gateways can also be used to collect data on a local level then manage the connection to a cloud server for the transmission of this data. In this way, not every device or sensor must be connected to a cloud or network server.

### Wi-Fi
Wi-Fi, in general, is a technology that uses radio waves to transmit information at specific frequencies. It enables high-speed and secure communication between a variety of devices, without wires, over both short and long distances. More specifically, enterprise-grade Wi-Fi, in contrast to consumer-grade, provides a higher-level of service when it comes to performance, security, standards/compliance, and life-cycle management – factors that are important for connectivity in any IIoT system. The latest Wi-Fi devices using Wi-Fi 6 and 6E frequently support some of the most current security offerings, such as WPA3.

### Bluetooth
Bluetooth is a wireless technology that allows mobile Bluetooth devices to exchange data over short distances. The original classic Bluetooth was designed to continually ▶

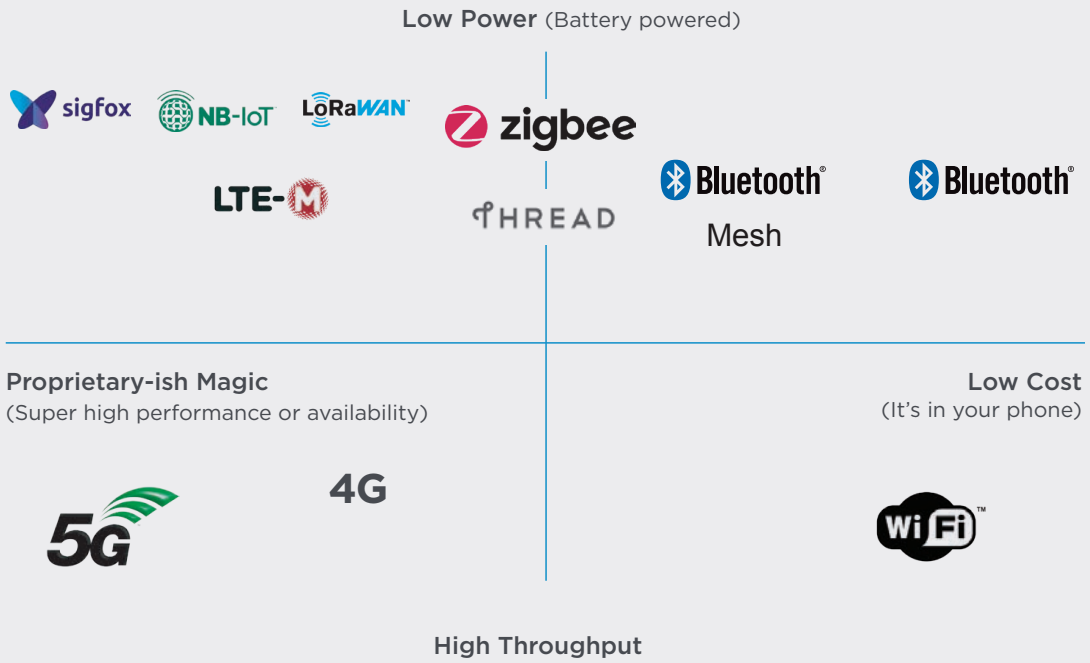



*Figure A*

**Figure 1** provides a basic overview of each of these wireless technologies in regard to cost, performance, and level of power and/or throughput. In general, low-cost versus high performance and low power versus high throughput.

stream data over short distances. Since its early days as a means to connect earbuds to your phone, Bluetooth has rapidly evolved as a low-cost, solidly performing option for wireless sensor applications.

The more recently developed Bluetooth Low Energy, also known as BLE or Bluetooth LE and introduced in Bluetooth 4.0, is a low power yet robust technology intended for situations where battery life is more important than high data transfer speeds.

Bluetooth 5 introduced a popular new feature called the LE Coded PHY. Use of this technology can provide up to four times the range as previous versions of Bluetooth, at the cost of a lower data rate. This trade-off has proven a popular choice for battery-powered wireless sensors.

Adopted in 2017, Bluetooth mesh is a networking Bluetooth technology that replaces the one-to-one Bluetooth exchange with a many-to-many relationship between Bluetooth devices. Mesh networks, in general, can effectively meet communication requirements over large areas while monitoring and managing many devices. Bluetooth mesh networking, more specifically, accomplishes these things while also maintaining compatibility with current devices and, because it depends on Bluetooth LE technology, does so with low-energy efficiency.

## LPWAN

Rather than being a single technology, low power wide area network (LPWAN) is a broad term to describe a group of protocols that operate using low powered devices to communicate small amounts of data over long distances.

There are several technologies competing within the LPWAN realm including LoRaWAN and cellular protocols such as LTE CAT-M1 and narrowband IoT (NB-IoT). With some applications, using a LPWAN protocol like LoRa operating in the 900 MHz range allows greater range and better propagation through various building materials than Wi-Fi or BLE. The cellular LPWAN technologies like LTE CAT-M1 and NB-IoT are becoming very effective in connecting remote sensor devices. These protocols are different from standard cellular services because they are meant to support low data rates at much lower cost than support for standard voice and data cellular service.

## Wireless gateways

Within the IoT, we are seeing growth in the adoption of gateway technology. A gateway is a physical device or software program that serves as a connection point between the cloud server/application and devices and/or sensors. All data moving to the cloud, or vice versa, goes through the gateway, which can be either a dedicated hardware appliance or software programme. Smart devices along with sensors can generate thousands of data points per second. With a gateway, devices can collect and pre-process or package the data locally before sending it on to the cloud. In this way, the end user can minimise the volume of data needed to be sent and can manage a secure connection through the internet and into the target cloud provider. Because the gateway manages information moving in both directions, it can protect data from leaks and IoT devices from being compromised by malicious outside attacks.

A gateway can support multiple connection technologies such as Wi-Fi, BLE, LoRa, Ethernet, and serial port ▶

connections. Most deployments use the ethernet or a Wi-Fi connection to the local area network as the doorway to manage the cloud connection. If using the local area network is not feasible, then a cell modem can be integrated into the gateway to utilise cellular connectivity to connect back to the cloud. The LTE CAT-M1 and/or NB-IoT service connections can be a cost-effective egress technology for lower data rate applications.

## Understanding telemetry vs. device management

It's important to understand the difference between two main functions of cloud services. The first is what we have been discussing for the majority of this whitepaper: getting data from devices and performing monitoring or analysis to create valuable insights and deep information. This is what we refer to as telemetry data. It is distinct from the second main function of the cloud, which is device management.

Device management is monitoring the status of devices in your cloud solution, including any error or debug information, software updates, provisioning and deployment, security analysis, and more. Where telemetry is interested in the data that applies to the application, device management is interested in the status and health of the sensors and gateways themselves.

## Selecting a telemetry system

There are many cloud solutions from which to choose once a business or manufacturer has a clear understanding of their specific telemetry needs. Even though most major cloud IoT platforms have a proprietary element to them, not choosing one is not really an option due to the fact that cloud-based services are a must for the vast majority who manage a connected IoT system. Also note that choosing a proprietary cloud solution is a far better option than trying to build your own. Even **GE**, in its financial prime, failed to develop a cloud platform despite investing billions of dollars.

The following are some important factors to consider when selecting a cloud platform.

**Who offers compelling IoT, analytics and machine learning capabilities?** While technologies such as message queueing telemetry transport (MQTT) are frequently available on nearly any IoT platform, edge and container technologies, robust database options, analytics tools, and particularly machine learning and artificial intelligence are not universal. Some platform providers are ahead of others.

**Which cloud platform will reliably still be around in five or ten years?** Longevity is important when it comes to producing and marketing stability to ensure a product's lifecycle can be supported. Companies in general are not permanent nor are they static and this applies equally to cloud solutions. Companies can go out of business or simply change their strategies or services which has the potential to disrupt critical day-to-day data management.

**Which cloud service provider is adding new features and additional capabilities more consistently or rapidly?** Technology is always evolving. New ideas lead to new features at a fast pace. To ensure an IIoT system is utilising the most advanced capabilities is important especially considering the pressure to outperform the competition as well as increase revenue and profit margins.

Although most major cloud IoT platforms have a proprietary element to them, not choosing one is not really an option due to the fact that cloud-based services are a must for the vast majority who manage a connected IoT system.

**How many devices will be connected to the cloud solution?** How much data will the cloud solution be managing? When selecting a cloud service, it's important to understand both the devices the manufacturer needs and the data that will be transported to and stored within the cloud. Scalability is the ability of an IIoT and cloud system to grow and successfully manage the increased demands of this growth. This is one of the most important features to consider with a cloud solution and a company's failure frequently comes from an inability to successfully scale up or down to meet its changing business needs.

**Which cloud service provider offers the most solid technology and development ecosystem and partnership for the business?** As noted in this paper, the implementation of an industrial IoT system is complex and challenging. It involves creating the appropriate connectivity architecture, managing regulations and security, as well as other vital considerations. It only makes sense to choose a cloud solution that offers the advance knowledge and experience as well as strong partnership to ensure an IIoT system's success.

## Selecting a device

*Management solution*

In addition to finding the right telemetry partner, finding a fully-featured device management solution is critical not just to the reliability of your devices, but getting them into the field in the first place.

Device management begins with a comprehensive security architecture, continues through deploying and provisioning devices remotely in the field, and continues throughout the life cycle with vulnerability monitoring and security updates. A fully-featured device management solution needs to stay in step with real-world threats, and ensure that devices are checked against security issues and provided with over-the-air fixes as needed. ▶

The following are important questions to ask when choosing a device management solution:

**Does your chosen partner meet or, ideally, exceed legal security requirements and regulations?** For an IIoT system to be deployed successfully and effectively, it must be deployed securely. As the move towards IIoT systems continues to grow along with the ongoing rapid influx of global connectivity, security becomes a greater challenge. Along with cybersecurity concerns, understanding laws and regulations regarding cloud-based data adds another layer of complexity to the business equation. Not only are regulations forced to evolve along with technology, laws also differ from country to country which adds to the difficulty.

The right cloud solution for a manufacturing IIoT system can not only help navigate these regulations, but it can also ensure the tightest possible security and over-the-air (OTA) security updates.

**Does it scale?** As we previously mentioned, failure often comes from an inability to scale an IIoT system to match business growth or, when applicable, business downturns. It's one thing to manage a system that includes a few connected IoT devices and a local cloud, but it's a far different matter to deploy and maintain a largescale IIoT system in a challenging environment with an increased criticality of connectivity and data delivery. Not only is scaling a system expensive, it also requires additional resources and technical know-how. For OEMs and other manufacturers, trying to accomplish this internally, versus provisioning from an external cloud solution partnership, often leads to IIoT business failure.

**Is it extensible to integration with your telemetry solution?** Not all cloud solutions play nicely with each other. In general, the largest telemetry platforms, like **AWS** and **Azure**, are dominant enough in the marketplace that third party providers' software can be integrated into their toolkits. However, as previously discussed, with this comes a requirement for significant development on the part of the OEM.

**Does a native device management platform already exist for the devices you're using?** In the classic build vs. buy decision, the convenience of relying on an existing device management platform can save OEMs significant development efforts, given that the platform meets the previously discussed requirements.

**Laird Connectivity**'s Canvas Device Management platform, which is already available for the IG60-BL654m BT610, and MG100, is powered by partner **EdgeIQ**. The device management platform simplifies workflows for configuration and maintenance of IoT device deployments. Easily set-up your devices, monitor performance, and keep software up-to-date across your entire IoT device fleet.

Laird has partnered with EdgeIQ and other industry leading cloud-based and SaaS providers, so that our customers do not need to integrate multiple third party components themselves. We've bundled everything together to fully integrate with your network infrastructure. Benefit from remote firmware updates, remote configuration and remote device health monitoring, all with seamless operation of Laird Connectivity sensors and gateways.

## Conclusion

It's understood that manufacturers are increasingly under pressure to encourage business growth by improving efficiency, decreasing operational costs and strengthening customer relationships. It's also understood that an effective IIoT system and the resulting data can vastly transform a business. As we stated earlier, despite the fact that IIoT systems are complicated and difficult to manage, the adoption of this technology across industries, including manufacturing, continues to increase at a rapid pace.

Simply put, don't try to rebuild what already exists. Find an IoT and cloud solution partner who can help make the best technology decisions for your IIoT system, allowing you to focus on your areas of expertise and getting the value out of the IoT data the system provides.

# The results are in - the second edition of the world's largest cellular IoT connectivity survey is complete

Results of Kaleido Intelligence's IoT Connectivity Survey show that complexity and consistency are key issues to solve

Following on from a comprehensive study completed in 2022, the second edition of the largest-ever survey of cellular IoT connectivity, commissioned by **Kaleido Intelligence**, is now complete. Surveying 800 IoT professionals, it investigated the most important factors for IoT connectivity firms to provide, as well as uncovering pain points for both those currently deploying IoT and those looking into it for the future.

The survey is one of the most far-reaching of its kind, covering topics such as how IoT projects are managed, the biggest concerns, and what they need from IoT service providers. In addition, we also examine the drivers for adoption of a range of promising technologies, such as embedded SIMs (eSIMs) and private cellular networks.

## 3GPP standards and support for international deployments biggest challenges

It is well understood that the cellular ecosystem does not provide a plug-and-play market for customers wishing to utilise the technology for their connected device programmes. Projects are often bespoke, with specific outcome requirements according to the enterprise customer. Here, the survey underlined how both cellular IoT adopters and non-adopters view the complexity of cellular connectivity standards in addition to a challenging environment where international IoT deployments are required as key pain points.

3GPP standards mean that organisations developing IoT programmes using cellular technology must grapple with an elaborate set of protocols, specifications, radio access technologies, ▶

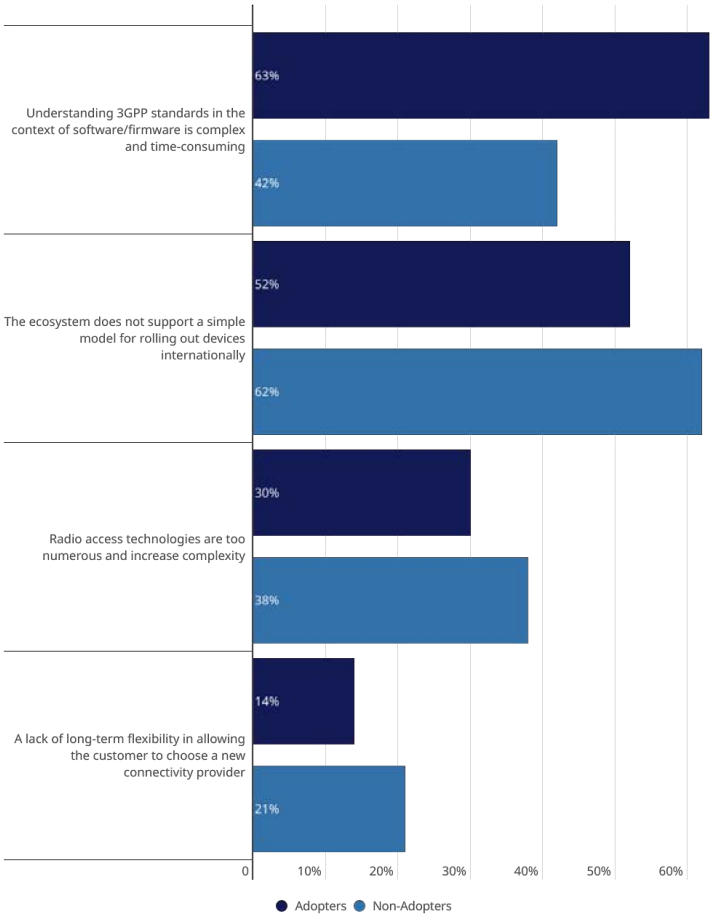



**Figure 1: What do you perceive as the main challenges for organisations wishing to use cellular technology for IoT for the first time?**

interoperability concerns and technology capabilities, requiring a high level of expertise in order to generate positive outcomes from their IoT projects. Certainly, it is evident that support from connectivity service providers is needed here to smooth the path to both adoption and the ability to scale deployments up.

Meanwhile, the nature of the ecosystem means that where international connectivity is required, customers must often engage with multiple connectivity service providers in order to meet requirements in terms of coverage, performance and price. In turn, this introduces challenges in the form of commercial and technical complexity for back-office operations and can mean that scaling up is difficult. While technologies such as eSIM and the emerging bring your own connectivity (BYOC) concept aim to help solve some of these challenges, it is evident that there remains much work to be done.

## A call for harmonised customer service and professional expertise

The results above were further underlined by the study, with 60% of respondents citing a lack of global adequate customer support and a lack of expertise to simplify the IoT journey for customers, reported by 56% of respondents.

Unavoidably, the need to engage with multiple providers across countries and regions where connectivity is required means that support levels cannot reach a consistent level wherever devices are located. In some cases, this means that support and incident resolution times are protracted, damaging the viability of the IoT deployment.

Overwhelmingly, complexity was uncovered as a key theme from the survey, and this was reflected by respondents calling for additional aid in helping them navigate the industry for their projects.

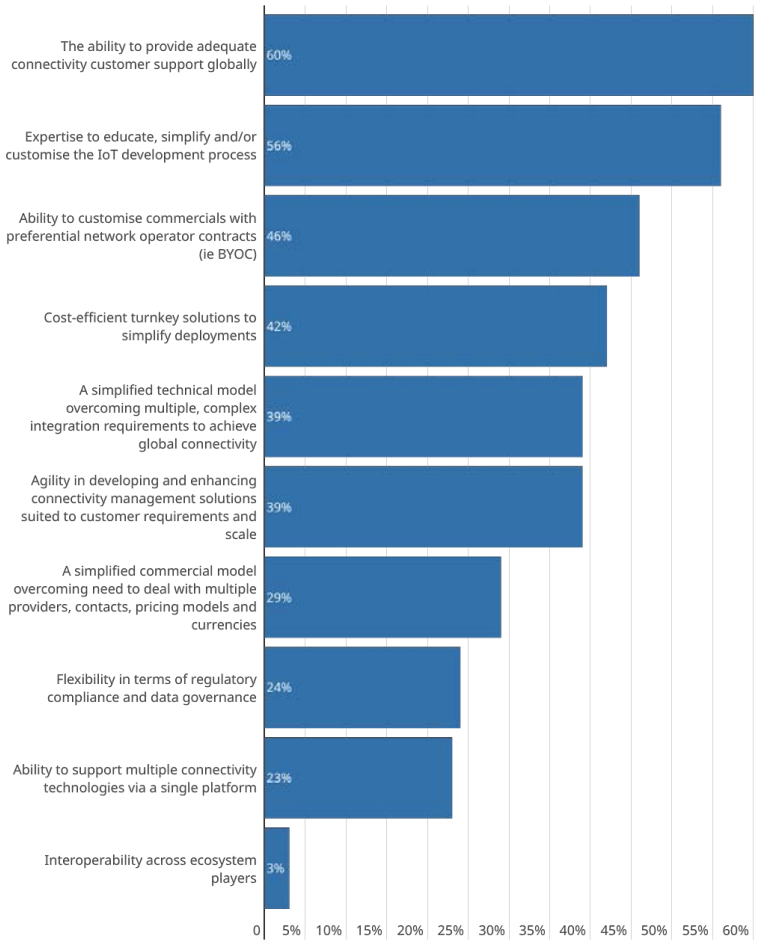
## Join the webinar

The survey findings will be presented and discussed in detail during a webinar on 24 May at 15:00 BST. The insights will be presented by **Kaleido Intelligence** and a range of industry leaders, including **BICS**, **Pod Group**, **Kigen** and **Pelion**.

Join us for the webinar and receive an exclusive free whitepaper detailing the results by signing up here.

If you are unable to join us, please register here to receive access to an on-demand recording following the event, and the accompanying whitepaper.

**Figure 2: What do you perceive as lacking in the present IoT connectivity ecosystem?**




## About Kaleido Intelligence

Kaleido Intelligence is a specialist consulting and market research firm with a proven track record of delivering telecom research at the highest level. Kaleido Intelligence is the only research company addressing mobile roaming in its entirety, covering:

- Data Forecasts by Market
- Historical & Forecast Viewpoints
- Competitive Intelligence
- Strategic Insight
- Trend Analysis

Research is led by expert analysts, each with significant experience delivering telco research and insights that matter.

# New report explores radical changes in the IoT connectivity management platform landscape

New position paper from Transforma Insights identifies how an evolving toolset and changing economics are transforming the connectivity management platform (CMP) landscape. Matt Hatton, the founding partner of Transforma Insights, shares the key findings

**Matt Hatton**
Transforma Insights

IoT analyst firm T**ransforma Insights** recently identified a series of ten key aspects of the Internet of Things that are going through a period of seismic change, technically, commercially and operationally. These IoT 'Transition Topics' include device/connectivity bundling, embedded SIM (eSIM) and localisation, and regulation. The first topic to be addressed, with a new Position Paper, is CMPs and the fundamental changes happening in their functionality, economics, and market dynamics.

## A changing of the guard?

The CMP is one of the key underlying pieces of middleware that mobile network operators (MNOs) and mobile virtual network operators (MVNOs) use to manage connections, handling activation/deactivation, billing, analytics, reporting and various other functions. If we look back 3-5 years, the CMP space was relatively stable. The functionality included within CMPs was well-established and the market landscape well defined, being dominated by two large players, **Cisco** and **Ericsson**.

***The IoT connectivity market is bifurcating, with one market focused on high-end, high-bandwidth, high revenue, connections (such as automotive), and the other focused on low-end, low-data, low revenue***

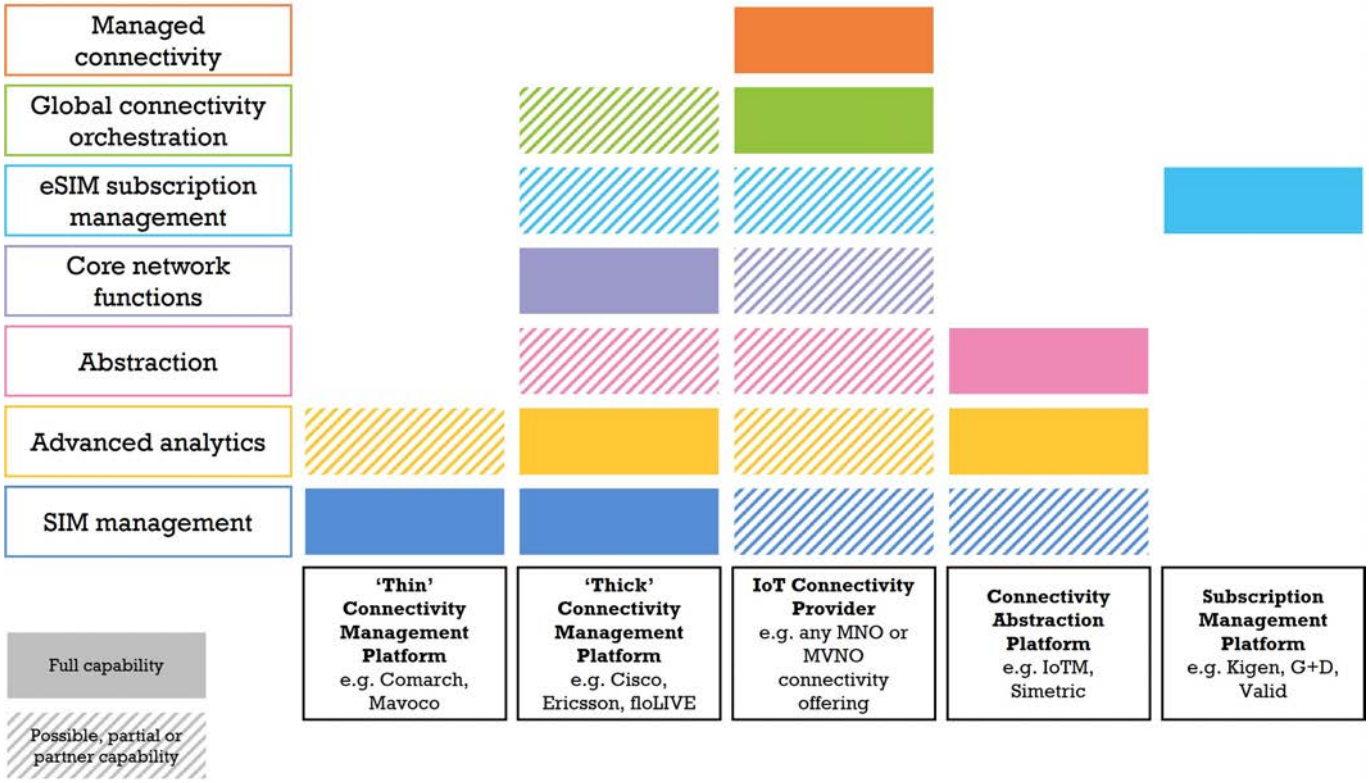
However, fast-forward a few years and we are in the midst of a pronounced transition phase. The biggest piece of news in the IoT connectivity space for many years was announced in December: **Aeris Communications** would acquire the IoT capabilities of Ericsson, predominantly its Connectivity Management Platform, IoT Accelerator (IoTA). Ericsson is one of the 'big two' in the CMP space, along with Cisco's Control Center. Cisco has also been through something of a transition in recent years with some price changes that weren't always welcomed by their mobile network operator customers. At the same time, alternative vendors such as **1oT**, **floLIVE** and **Mavoco** have come to market with agile cloud-native offerings with strong functionality delivered in a very cost-effective manner.

## The economic reality of IoT connectivity

There is a definite economic angle to these changes. Connectivity providers are wrestling with the challenge of what Transforma Insights refers to as '$1 IoT', i.e. how to support connections in a cost-effective manner when they generate average connectivity revenue of less than US$1 per year. This challenge is only going to become more pronounced with the increasing prevalence of narrowband IoT (NB-IoT) and LTE-M connectivity, addressing more use cases that generate very small amounts of data, and therefore revenue. The CMP offerings used by these connectivity providers need to adapt to reflect this. The question for CMP vendors is: how can they continue to support operator customers at declining revenue per connection, sometimes as low as US$0.20/year, at the same time as supporting their complex requirements, and all against a background of being essentially loss-making. Cisco has opted for a dual approach, raising prices to make its Control Center business profitable, and at the same time introducing additional value-added features and tiering. Ericsson has opted to exit the market altogether, transferring its IoT Accelerator business to Aeris Communications.

The tiering approach is certainly a necessary one. The IoT connectivity market is bifurcating, with one market focused on high-end, high-bandwidth, high revenue, connections (such as automotive), and the other focused on low-end, low-data, low revenue. The former can continue to be addressed using existing processes and platforms, albeit that a bit of streamlining wouldn't go amiss. The latter, however, probably needs a rethink, to ensure that it can be addressed profitably. It needs its own channels, processes, and perhaps a separate lower-cost CMP. The established vendors have recognised this dynamic. Cisco Control Center ▶

**Figure 1: Connectivity management platform variants**
[Source: Transforma Insights, 2023]




now comprises three levels: Advantage, Essentials and Lite. Similarly, other vendors such as **Comarch** and **Mavoco** have tiered offerings too.

## Differentiating thin and thick CMPs

Even more fundamentally than just tiering, the very concept of what defines a CMP has changed. There is a baseline set of functionality involving SIM management which is common to all CMPs, including activation/deactivation/suspension of the SIM, APIs and billing. Additionally they have varying levels of data analytics for anomaly detection, bill prediction and so forth. However, increasingly there is a split between those CMP vendors that only provide the basic functions (what Transforma Insights refers to as thin CMPs) and those that have enhanced it with a broad range of other connectivity-related functionality (the thick CMP). Cisco, for instance, talks now about IoT-as-a-Service rather than CMP, reflecting that the portfolio of offerings is now wider.

The thick CMP covers adjacent areas of providing core network infrastructure, analytics, eSIM and remote SIM provisioning (RSP) and some aspects of global connectivity orchestration, i.e. aggregating multiple connectivity provider offerings in order to present to enterprises. The key question for this segment is the extent to which it will be able to truly orchestrate the connectivity offerings of its operator customers, even potentially to the extent of providing a managed connectivity offering. Both Cisco and Ericsson have dabbled in this area in the past but have generally been dissuaded by their operator customers from pursuing it. However, the market may have moved on.

## MNOs weigh their options on CMP

Against this background, many MNOs are considering their strategic approach to CMPs. Should they stick with their existing long-established vendors? After all, they are still considered, particularly Cisco, to have market-leading functionality. Or do they shift to a new vendor such as floLIVE? This question was probably the number one topic of conversation at Mobile World Congress in February.
We are currently in a period of transition with ownership, functionality, market structure and buying behaviour all in a period of flux. Ultimately, 3-5 years from now we expect there to be a new normal in CMPs based on a more pluralistic market structure, with a wider range of, in many cases very feature-rich, platforms.

If you are an MNO considering its options on connectivity management platforms, we recommend tuning in for the Transforma Insights webinar on 16 May 'The future of IoT Connectivity Management Platforms in an era of transition', where Transforma Insights will be joined by Nir Shalom, the chief executive of floLIVE, in addressing all of the issues raised in this article, and many more. ■

***We are currently in a period of transition with ownership, functionality, market structure and buying behaviour all in a period of flux***

**www.transformainsights.com**

# Practice makes perfect for IoT security

IoT security is a priority for organisations of all types as they deploy IoT devices, applications and services. Matt Hatton, the founding partner of Transforma Insights, spoke to Simon Trend, the chief technology and services officer, and Paul Bullock, the chief product officer, of Wireless Logic to understand how the challenges are being overcome

***We think of the degree of risk and type of risk***

**Matt Hatton: Is IoT security more of an issue now than it has been in the past?**

**Simon Trend:** The cybersecurity threat from both state sponsored and criminal elements is more real than it's ever been. Given the scale and relative complexity of IoT systems – devices, networks, cloud, people, third parties and suppliers – the attack surface can be vast. Automation tools which probe for weaknesses are more readily available, social engineering can be effectively deployed against organisations. We have new legislation. So yes, security is more of an issue. I would also add that the speed of growth of the IoT market has outpaced the abilities of the technologies to keep it secure. I think there's been an element of catch-up from the providers in being able to address the specific needs of IoT and only some providers are closing that gap in an economical way.

One example of IoT economics would be licensing costs. Traditional security companies offering endpoint detection and response technologies are quite capable of working with IoT data sets, but the licensing is massively prohibitive. You can't afford to spend US$20-$30 per device on IoT applications.

**MH: Is there such a thing as too much security?**

**Paul Bullock:** If we ask what's keeping CTO/CISOs awake at night? If you're running an IoT solution or you're an original equipment manufacturer (OEM), security is probably one of the biggest things. That awareness, with everything going on in the world and geopolitical risk, means I think people have more visibility and that could lead to some overdoing it.

We think of the degree of risk and type of risk. If you have a wearable diabetes monitoring device pushing very personal data, it's a different level of risk from a pH or moisture sensor. You have to look at the degree of risk based on the type of data and think about potential risk in terms of implications. Is it around sensitivity of data? Is it a commercial fraud risk, for instance for payment systems? Is it a safety risk where you have a lone worker device that's not working? Or is it reputational risk? ▶

**Simon Trend**
**Wireless Logic**

**Paul Bullock**
**Wireless Logic**

You need to balance the security provisions you're putting in place against effectiveness, usability or the commercial viability of a solution. You can't spend US$40 on a device or solution that generates US$10. The economics are really important. We definitely really encourage customers to think about the degree of risk and apply security appropriately.

Also to build security techniques and costs into the solution to the highest degree possible to improve operations and solution delivery. When you can save money on a secure element, when you can auto-register to a cloud target and achieve cloud portability while managing the identity of devices yourself, that knocks a lot of things on the head.

**MH: How do you view initiatives such as IoT SAFE?**

**PB:** Identity is fundamental to security. Building that in and being aware at the point of manufacture and certainly at the point of connectivity, you've established identity. It's immutable. With **AWS** once the software developer kit (SDK) is on your device you're never leaving. Using IoT SAFE means you have the ability to have a hybrid cloud environment because you're in control of your device identity. And also, you have an opportunity for portability and evolution of your solution between clouds over time. It's improving your cost control by giving you the chance to add a new cloud target in the future. You're keeping the keys to your own car, for a very nominal amount of money.

In terms of the component cost savings, saving a dollar is meaningful in the IoT device. That comes from not having a dedicated secure element or an embedded Flash device. We have experience where customers were taking that embedded Flash approach and were emailing their keys to their third-party contractor for install. I don't think they ever had an issue but the risk was huge.

**ST:** IoT SAFE also achieves standardisation, which is important, to allow broader adoption of edge security and identity. Up to now it has been very proprietary and it's hard to build a product with confidence that it will work everywhere. If you meet security at the edge with something which is standards- ▶

***"We recommend that businesses adopt a security framework approach and consult closely with a tight group of trusted partners"***

based and allows very careful identification of the device you reduce the need to monitor everything in order to spot anomalies.

We hear the phrase 'secure by design' a lot. It's important to know what is meant by it. For us you need to really think about security in the device at the ideation stage. It's much more difficult to add secure components later once you've gone from design into manufacturing. That's what we mean by secure by design: consultation at the ideation stage and really designing these elements into your solution.

**MH: What practical steps are the most obvious for enterprises and OEMs to head off the biggest security risks?**

**PB:** We recommend that businesses adopt a security framework approach and consult closely with a tight group of trusted partners. It's how we like to operate. Our framework is built around a series of 16 defend, detect and react provisions. It covers technology of course but also people and processes. Secure device identity and comms are strong foundations but the ability to detect and react quickly to breaches is just as important.

There's a differentiator for us here, with IoThink Solutions. It's our digital twin platform covering 1,200 devices and counting, where we're positioned in the market with IT/OT organisations in energy, manufacturing, building and enterprise sectors. Customers can model their entire solution in software. They can see the real behaviour of the systems and optimise end-to-end. So everything can be thought through and visualised properly before going into the field.

**ST:** Bringing it back to security by design, some customers might think you progress from a virtualised version to a physical thing and then you secure and optimise that. IoThink has evolved to be an integral part of the change development, planning and everything that happens to that stack of technologies that you're working with. It's not where you originally deployed the application, it's that patch, that update, that adjustment that's made. That's where the mistakes happen and where security holes creep in. So it's a continuous process of retesting, remodelling the data and how the applications are configured that's really where we make security happen.

**MH: What about people and training?**

**ST:** You need to involve the employees in your organisation in what you're trying to achieve in security. It might sound trivial, but something like 90% of breaches are due to people. At the centre has to be a security mindset. That will drive the right processes, designs and implementations. Outsourcing is one thing, but you need to bring in your own employees who know the industry and the company and then bring in the security training and capabilities and add to it. The employees form the best line of defence in any organisation, irrespective of any investment they make.

There are some questions businesses should ask themselves: Who in the senior management of the organisation is accountable for security? And who is the person that's responsible for embedding a culture of security? And what are you doing to simulate challenges and learn from them?

I'm also quite keen to reflect on things that you can do which are perhaps new. We've talked about white hat hacker programmes for years. Platforms like **Intigriti** and **HackerOne** provide access to thousands of researchers. Nothing beats 1,000 people trying to find a vulnerability because one of them will get through. It helps organisations understand that they're properly secured, dealing with that extra 1-2% they can't cover internally.

**MH: Any other ways the threat landscape has evolved in the last few years? Types of threats, regulation, different actors?**

**PB:** The automation of cyber-attacks and the prevalence and ease of setting up a cyber-attack with multiple facets has never been easier. Imagine a ChatGPT type instrument pointed at cyber-attacks. And that could be twinned with social engineering and brute force attacks.

**ST:** In terms of regulation, there are areas where the UK, in particular, is leading the world on IoT security. They are taking the steps others have spoken about. If other countries follow at a similar pace, the potential attack surface of IoT solutions and the risk from the threats that everyone perceives will diminish.

**PB:** Further on the legislation and regulation, it's starting to get some teeth, which is a good thing. You could argue that different regions and countries having different legislation could be an issue for global IoT although they could all adopt a common set of standards, for instance based on **ETSI**. Even if legislators have a consumer focus, it makes sense for enterprise buyers to insist that devices and solutions are compliant with best practice.

Security is an ongoing exercise that needs to evolve as threats evolve and new tactics are adopted by hackers. Just because you're certified once it doesn't mean you'll be compliant next week. So, regulations and ▶

standards are a really good thing but on top, there needs to be a framework for constantly monitoring and evolving your security policies and defensive measures.

**ST:** Another dimension is that practical threats are a lot lower level. Companies looking to extract thousands rather than millions from companies. A lot of these companies have call centres, they have agents who can help take payments for ransomware, they can even troubleshoot issues for unlocking your data. Ransomware insurance is an option for businesses. It's at an industrial scale.

**MH: What are the trends in the cost of security?**

**ST:** The cost of connectivity globally has declined substantially to sub-$1 anywhere in the world, but you still need to overlay security and support services. Companies will pay it somewhere else, for instance having to invest in new technologies in the core which are there only because your connectivity provider, while cheap and cheerful, isn't providing the fundamental basics. The cost of security is going to have to be reflected in the cost of connectivity.

**MH: Is this about enterprises having a single security partner?**

**ST:** Organisations need to carefully select from suppliers that have already pre-integrated at different levels and will offer a reduced amount of noise and inputs for them to be looking at. That's where **Wireless Logic** is investing. To combine things together to provide a single source for some of the security aspects around connectivity, leaving organisation to invest in things to do with the application, corporate security and the data.

Is there one provider to provide all security services? No. But there's a lead vendor with an ecosystem of partners that can coordinate with a framework approach.

**MH: We all work in the Internet of Things where the concept of automation is core to what we do. How much of IoT security should be automated?**

**PB:** Automation should help with detection and reaction to any breach but it probably needs people and knowledge as well. By modelling with IoThink, we see how things adapt to events, to understand what's normal and what's an anomaly. You can use that system to start to automate. The time to detection is probably directly proportional to the cost and damage of any breach.

You can see the picture we're painting. Anomaly detection, plugged into Conexa, our mobile core network that we have built specifically for IoT, building a view of devices in the field, up to IoThink, that has already digitally twinned all the devices and is managing them in the field and ingesting the data.

**ST:** One thing we haven't talked about is rehearsal. Ultimately detection and analysis is all useless if you don't rehearse it. It's not if, but when, you get breached. And when you do, the speed of response is more important than anything else. Rehearsal of scenarios around security have a huge bearing on the speed with which you can respond. RanSim simulates 22 types of cybersecurity, which helps you rehearse the basics of how to respond to a ransomware situation. That rehearsal helps the speed of response. And it's that speed that's the only thing that people can improve, since it's inevitable you'll get breaches.

Anyone with security responsibilities will be continuously assailed by pressure from new threats, output from their own application stack, with increasing frequency and richness. It's a lot to digest. Focusing on fewer organisations that are pre-integrating a lot of that data and automating a lot of decisions and analysis about it is quite important to reduce information overload. ■

***The cost of connectivity globally has declined substantially to sub-$1 anywhere in the world, but you still need to overlay security and support services***

**www.wirelesslogic.com**

# TRANSFORMA INSIGHTS

## Global Advisors on IoT and Digital Transformation

## Leading the conversation on IoT

Transforma Insights is the leading analyst firm for the Internet of Things, setting the standard for qualitative and quantitative market research.

What makes us different from other analyst firms?

- **Focus:** We focus on the impact of key disruptive technologies, including the Internet of Things and AI, that will change how enterprises operate.
- **Access:** Our analysts have unrivalled access to key executives at the leading technology vendors and innovative start-ups.
- **Immersion:** We engage more with the ecosystem, speaking at conferences, judging awards, and meeting face-to-face with people that matter.
- **Granularity:** Our research digs deeper into our areas of coverage, for instance our ultra-granular market forecasts.
- **Depth:** Our analysts are thought-leaders in the technology space, authoring cutting-edge research.
- **Rigour:** Our research is backed by extensive primary and secondary research including extensive surveys.

Sign up to your free 'Essential' subscription to explore our research at: transformainsights.com/signup/essential

transformainsights.com enquiries@transformainsights.com @transformatweet

## IoT SECURITY-AS-A-SERVICE

# Why enterprises need IoT Security-as-a-Service

SPONSORED BY

wireless logic

**Matt Hatton**
**Transforma Insights**

# Why enterprises need IoT Security-as-a-Service

The rapidly evolving IoT security threat landscape necessitates enterprises finding trusted partners to mitigate risks across the endpoint, network, transport, cloud/data and application layers, writes Matt Hatton, the founding partner of Transforma Insights

This report provides enterprises with a view on the evolving IoT security landscape and the best mechanisms for mitigating the risk and impact of security threats. It starts with the results of **Transforma Insights**' recent IoT Connectivity Survey, demonstrating how critical security is considered to be. The following sections examine the ways in which the security threat is evolving, a dive into some of the legislation affecting IoT security, and a topology of IoT security, identifying the various types of security requirements. The final sections provide enterprises with a guide to how security considerations need to be stitched into their IoT deployments, and an explanation of why Transforma Insights believes that there is a need for something called IoT Security-as-a-Service to mitigate growing and evolving IoT threats. ▶

## Key messages

- IoT is complicated, with many moving parts spanning multiple different disciplines (e.g. device, cloud, transport, and network), all of which have their own special security considerations.
- IoT security risks are evolving fast making it increasingly challenging for enterprises to stay on top of them.
- The regulatory landscape is particularly moving fast at the moment, with new rules and regulations emerging every year.
- IoT security must consider all of the constituent parts of the solution holistically; a chain is only as strong as its weakest link.
- Enterprises must conduct due diligence on their suppliers. Your security is only as good as that of your suppliers.
- The optimum approach for many will be to find a trusted partner, delivering IoT security as a managed service.
- Enterprises will never completely remove risk. There will always be breaches. A good strategy includes serious consideration of remediation after breach.

## Enterprise perspectives on IoT security

Security continues to be one of the top requirements for enterprise IoT buyers. According to a survey conducted by Transforma Insights in September/October 2022 of more than 1,100 buyers of enterprise cellular-based IoT connectivity, security was the number two factor influencing the choice of connectivity provider.

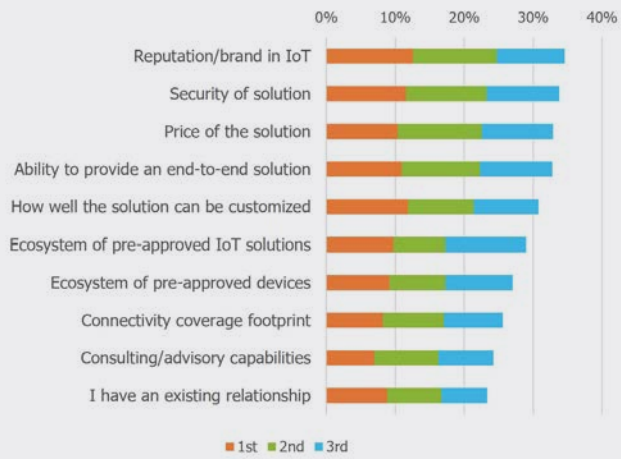
As illustrated in **Figure 1**, it was 'reputation/brand' that was the top choice, indicating that there is a gating factor for vendor selection which first considers which providers are reputable and reliable before going on to consider topics such as security and price. However, security considerations would likely also be part of the thought process of determining which providers would be deemed to have a good reputation.

Digging into the topic of security in a little more depth, as we do in **Figure 2**, we can see that the importance of security varies in a quite marked way depending on the geography, sector and size of the organisation.

While a total of 34% of respondents quotes security as being one of their top three considerations, this was as low as 23% for the utilities/energy vertical and as high as 36% for the public sector. The low rating in ▶

**Figure 1:**
**Top factors influencing choice of vendor, 1st, 2nd, 3rd choice**

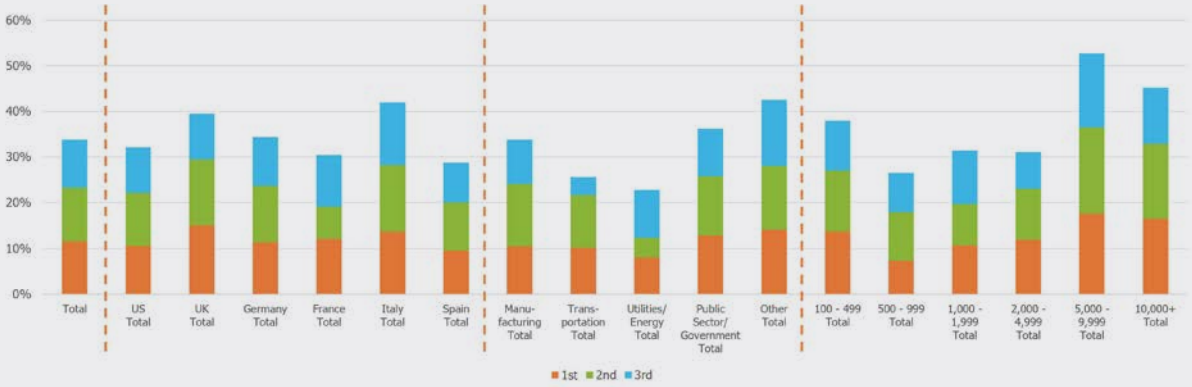
Source: Transforma Insights, 2022




What are the top factors that would influence you to select a particular IoT solution provider?
(n=1,114)

**Figure 2:**
**Top factors influencing choice of vendor: Security of Solution, 1st, 2nd, 3rd choice**

Source: Transforma Insights, 2022




What are the top factors that would influence you to select a particular IoT solution provider? "Security of solution". (n= 1,114, US 510, UK 119, Germany 131, France 115, Italy 124, Spain 115, Manufacturing 237, Transport 176, Utilities 185, Public 163, Other 353, 100-499 211, 500-999 257, 1,000-1,999 290, 2,000-4,999 209, 5,000-9,999 74, 10,000+ 73)

the utilities/energy sector is perhaps surprising given the fact that it is heavily focused on critical national infrastructure involving applications such as smart metering and smart grid. Perhaps we can interpret it that they are at this stage comfortable with the levels of security they receive and have moved on to thinking about other topics. This is somewhat borne out by the fact that when asked in a separate question about demand for future features, respondents in that sector strongly favour lower prices as a priority rather than security.

As shown in **Figure 2**, there is also something of a trend for larger organisations to have a greater consideration of matters relating to security than their smaller peers. This might well reflect the fact that larger organisations are likely to deploy more critical use cases, whereas for smaller organisations there may be fewer threats. Or alternatively, it may just be that smaller organisations are more focused on just getting their IoT project off the ground.

## IoT security threat landscape

The security threats associated with the Internet of Things are growing. Enterprises are paying more attention than ever to how to mitigate the growing risk. Transforma Insights identifies ten key reasons why the threat from security breaches in IoT is increasing.

### 1. More use cases

There are more enterprises and consumers deploying IoT than ever before, opening up more potential hacking opportunities for bad actors. Consumer devices such as refrigerators, washing machines, ovens and lighting systems are increasingly shipping with connectivity embedded. Enterprises are finding more and more ways in which IoT can be useful for streamlining business processes or giving them a competitive edge, whether that be in supply chain, manufacturing automation, retail or any other vertical.

The democratisation of the use of IoT makes for a greater number of potentially vulnerable systems and endpoints. It also means that there is a great potential for losing track of legacy IoT deployments. Unlike most traditional ICT deployments, such as PCs, phones or servers, these IoT devices are usually unattended and will often be operating for decades without any need to replace them, or interact with them in any way. It's easy to lose track of every thermostat, security camera and water pressure monitoring device installed on your network.

### 2. Bigger scale

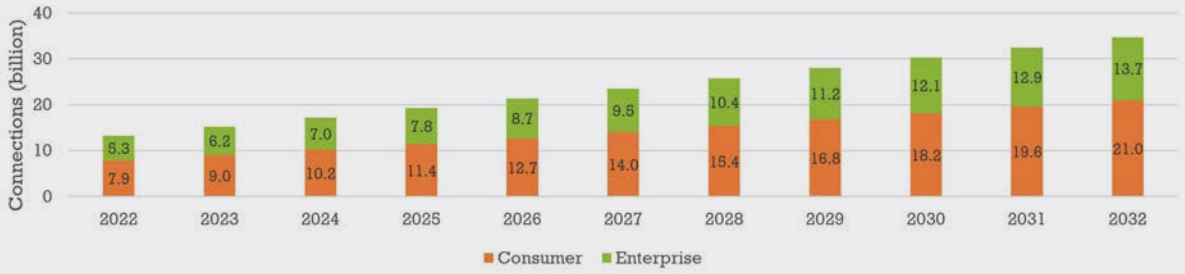
Hand in hand with the increase in use cases, the volumes are growing. At the end of 2022, Transforma Insights estimates that there were 13.2 billion IoT connections worldwide. By 2032 that figure is expected to increase to 34.7 billion. Simply by virtue of the growth in numbers of devices, the cybersecurity vulnerabilities are multiplied.

### 3. More mission-critical

According to a recent survey by Transforma Insights, enterprise IoT adoption is heading into a new phase ▶

**Figure 3:**
**Global IoT connections, 2022-32**

Source: Transforma Insights, 2022




whereby businesses are entrusting more critical core systems and processes, including those directly affecting their relationship with customers, to IoT.

The counterpoint to this use for more mission-critical systems is that such IoT deployments are more appealing for ransomware attacks, and more appealing to state actors looking to find vulnerabilities in critical national infrastructure. One good example here is the Colonial Pipeline hack of 2021, whereby a US oil pipeline carrying refined fuel was subject to a ransomware attack. The increasing use of remote management of such critical assets opens up the potential for attack.

### 4. Physical vulnerability

Many IoT devices are located remotely and almost all of them are unattended, i.e. there isn't someone constantly interacting with them. As a result, many classes of IoT device are more vulnerable to being accessed by malicious actors. A good example is the case of mobile-connected traffic lights in South Africa, where thieves broke into the connectivity units and stole SIM cards which were then used in other devices.

### 5. Constrained devices

One of the key IoT trends of the last decade, well documented by Transforma Insights, is the emergence of the 'thin IoT stack', which describes an emerging norm within the development of IoT applications to make use of specific off-the-shelf technologies that have been created explicitly to be optimised for use in constrained environments, the constraints being some combination of limited access to power, low bandwidth connectivity, and limited processing and memory.

One result of using these constrained technologies is that they often have limited capability to support security features. In some cases on-device processing is very limited, or networking protocols may not support the appropriate level of security, or the available data transmission may be so limited - due to the available technology or the desire to maintain battery life - that firmware updates are difficult to achieve. With the constantly evolving threat landscape it's critical to be able to do firmware over the air (FOTA) updates, which may not be possible with some constrained technologies.

### 6. Interconnectedness

An under-considered aspect of IoT security is the extent to which different systems make use of common infrastructure, opening the up to security vulnerabilities. The most common are man-in-the-middle attacks on users' Wi-Fi networks. These open up the risk of financial fraud and other serious issues. In one case, **Pen Test Partners** easily hacked an iKettle, to reveal the Wi-Fi password for the network on which it resided. The most famous example of this is probably the Las Vegas casino where financial details of customers were accessed by the hacking of a fish tank monitor. **Target** had a similar experience in 2013 when hackers made use of vulnerabilities in its HVAC system to access credit card information. And the famous **Jeep** hack of 2015 saw white ▶

**Figure 4:**
**Transforma Insights' ten reasons why IoT security threats are increasing**


hat hackers exploit a vulnerability in the infotainment system to get access to the CANBUS, allowing them to steer and stop the car.

### 7. Complexity

Any IoT project involves multiple participants and a diverse array of technologies, including device, network, application, cloud, enterprise back-office, end user and more. All of these represent potential weak-points. A chain is only as strong as its weakest point.

### 8. Diversity of devices

Managing security on IoT devices is an order of magnitude more complex than managing it for a limited array of traditional ICT devices, such as handsets, PCs and IT infrastructure. While handling device management in a bring-your-own-device environment was slightly challenging due to the variety of device types, with IoT that is expanded ten-fold. Enterprises need to consider security vulnerabilities of a diverse range of devices across generic IoT deployments, such as building automation or security, and specialist vertical use cases, such as process automation, payment terminals, track and trace or inventory management.

### 9. Lack of skills

There is a shortage of skills for developers in ICT in general and this is particularly pronounced in the IoT, where the set of capabilities required is very broad, spanning both hardware and software. Many security problems arise simply because the developer was not cognisant of the risks across associated domains with which they may not be too familiar.

### 10. Lack of regulation

This item could have been called 'manufacturer corner-cutting' because that's largely what stimulates the need for regulation. Hardware developers trying to produce as cheap a product as possible will often cut corners, and security is one of those corners. The Mirai botnet, for instance, which infected as many as 400,000 consumer IoT devices, particularly video cameras, was able to do so simply because of a lack of basic security on those devices. Regulation is needed to ensure they do not do that. ▶

### IoT security legislation

One of the key aspects of IoT is regulation. Over the last couple of years there have been some quite significant laws introduced in the US, EU and elsewhere covering IoT and particularly IoT security. It's critical to keep on top of the changes. The focus of regulation until very recently has been on providing voluntary guidelines for device manufacturers, but the coverage is expanding and the guidelines are evolving into concrete obligations in many cases. These are mostly consumer-oriented and not immediately applicable to B2B IoT, but they will become established best practice for any IoT deployment. Enterprises can and should be looking for vendors that are compliant with the salient parts of these regulations.

### The US

The IoT Cybersecurity Improvement Act, 2020 is focused on federal procurement of IoT but not private sector or consumers; although the aspiration is that federal procurement volumes will trigger changing behaviour by manufacturers more generally. It gives the National Institute of Standards and Technology (NIST) oversight of IoT cybersecurity risks, requiring it to set up guidelines and standards, including over reporting on security issues. NIST has a set of voluntary guidelines for manufacturers, which are promoted as capabilities consumers should look for, including a unique identifier and the ability to configure and update firmware.

On the 1 January 2020 California's Consumer Privacy Act came into force, regulating privacy requirements for Internet of Things (IoT) devices. It applies to any company that counts California residents amongst its customers. As a result, it is effectively a national – and arguably an international – law. Oregon introduced almost identical legislation on the 1 January 2020. The law covers any device that is assigned an IP or Bluetooth address and is capable of connecting directly or indirectly to the internet. Because it covers any device regardless of whether owned by an individual or a business, the law includes both consumer and non-consumer devices. The law is somewhat light on specifics, requiring ostensibly that an IoT device carries a 'reasonable' level of security that is 'appropriate' to the characteristics of the device and the information that it collects, stores or transmits. There are a few mandated requirements for devices connected via wide area networks. Each device must have either a unique pre-programmed password or must contain a security feature requiring the user to generate a new means of authentication before getting access to the device for the first time (i.e. the user be required to set a password).

### The EU

The EU Cybersecurity Act which came into force in 2020 placed a requirement on ENISA, the European Union Agency for Cybersecurity, to define a certification framework for ICT products and services, which was released in November 2019 as "Good Practices for Security for IoT – Secure Software Development Lifecycle". This focused on ensuring security is baked in to the software development lifecycle for IoT. However, it contains only 'good practices and guidelines' rather than regulations. This voluntary certification scheme will be reviewed periodically.

The EU Cyber Resilience Act was published in September 2022. It will address the current low level of cybersecurity within IoT devices and the need for software and firmware updates to patch vulnerabilities. Features will include minimum password standards, the ability to support software updates, some form of vulnerability testing and restrictions over the use of personal data. It will apply to manufacturers and developers across hardware and software and include substantial fines for non-compliance. It is likely to include requirements for providing buyers with greater product information as well as prohibiting the sale of devices that do not comply with requirements. After adoption by the EU there will be an implementation period by national governments, meaning that the obligations are likely to apply from some time in 2025. National governments are also able to apply their own national rules independent of those of the EU.

Other relevant regulations include the NIS2 Directive, introduced in January 2023, which is focused on encouraging member states to harmonise cybersecurity rules, examine current vulnerabilities, establish national cybersecurity strategies, and the wider General Data Protection Regulation (GDPR) which covers the use of personally identifiable data.

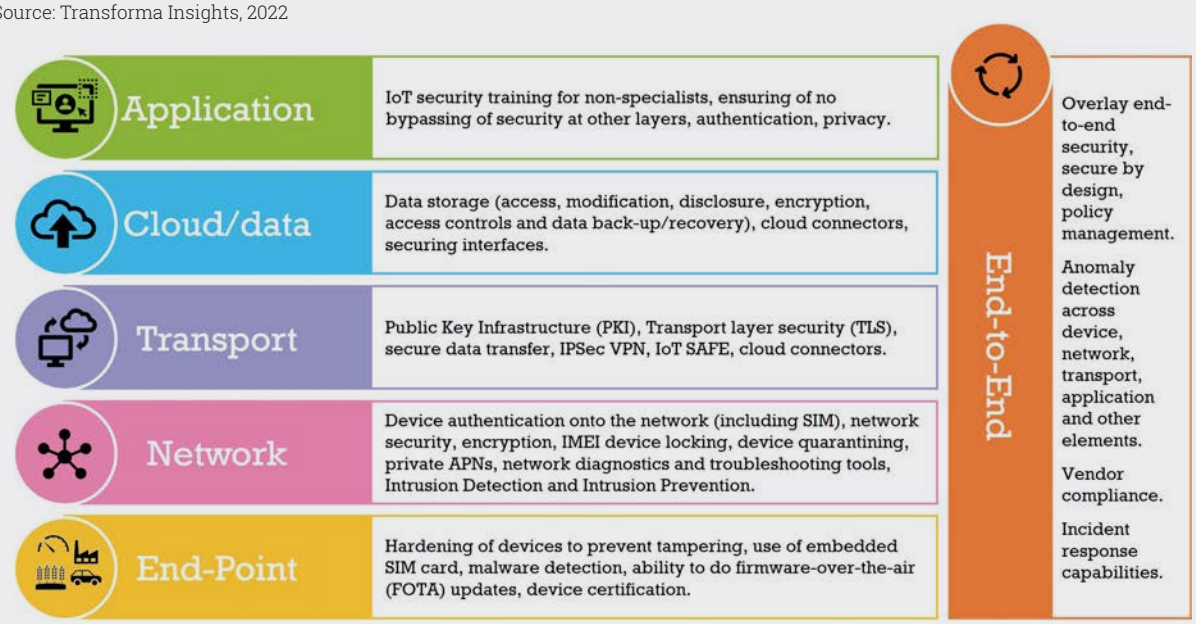
The European Telecommunications Standards Institute (ETSI) is a standards body rather than an arm of government and as such does not have legislative power. However, its Consumer IoT Security standard EN 303 645, released in June 2020, has 13 recommendations including no default passwords, a requirement for software updates and inclusion of features to allow users to delete personal data.

### The UK

At the start of 2020, the UK set out a Code of Practice for Consumer IoT Security, representing a progression from the initial voluntary approach. It focuses on consumer ▶

**Figure 5:**
**The six layers of IoT security**

Source: Transforma Insights, 2022




devices only, although there is reference to extending it to enterprise in due course. It is slightly more explicit than that seen in the US, with thirteen guidelines from the **ETSI** 303 645 standard, and three main requirements:

- IoT device passwords must be unique and not resettable to universal factory setting.
- Manufacturers must provide a public contact point as part of its vulnerability disclosure policy.
- Manufacturers must explicitly state the minimum length of time during which the device will receive security updates.

This is set to be superseded by the forthcoming Product Security and Telecommunications Infrastructure (PSTI) Bill, which places requirements on manufacturers and vendors of IoT devices to meet new cybersecurity standards. This includes provisions such as a requirement for transparency over features and functionality, better public reporting system for vulnerabilities, and a ban on universal default passwords.

## IoT security layers

What do we mean when we talk about IoT security? IoT deployments are relatively complex, comprising devices, networks, platforms, applications, enterprise back-office systems on so forth. We identify six main security layers.

### Endpoint

The first consideration in IoT security is likely to be the 'thing'. The top priority within devices will be hardening to prevent tampering. This applies both to the overall device itself, and to the specific case of the SIM card. The latest generation of embedded SIM, or eSIM, is soldered into the device to prevent its removal.

Within the endpoint/device category we also include having the capability to do FOTA updates. This necessitates having the appropriate network technologies to handle the required data throughput (many LPWA technologies will not be able to handle it), as well as the required storage and processing on the device.
From a device firmware security standpoint, at the device layer the main priority will be malware detection.

### Network

Network security is generally very good, particularly on mobile networks. But that is not to say that there aren't also vulnerabilities here. This is exacerbated for IoT applications that are supported over a number of networks and peering points, including the public internet.

Vulnerabilities, even in mobile networks, have been exploited, for instance by pinging the home location register/home subscriber service (HLR/HSS) to identify a device's location, or by enacting denial of service attacks via the HLR/HSS. ▶

Network security incorporates device authentication, including SIM authentication, and network encryption. We include here functions such as private access point names (APNs), network diagnostics and troubleshooting, international mobile equipment identity (IMEI) device locking (i.e. preventing a device from connecting to any other network), quarantining of devices, and domain name system (DNS) white-listing. Also anomaly detection might be done at the network layer too. In some cases, IoT connectivity providers deploy specific intrusion detection systems (IDS) and intrusion prevention systems (IPS).

### Transport

In many cases, enterprises deploying IoT will consider that network layer security alone is not sufficient. And furthermore, many cloud providers demand some transport layer security (TLS) for data delivery into the cloud. Typical approaches to TLS use a hardware security module (HSM) or cloud providers' software developer kit (SDK) on the device.

Features relevant here include the provision of IPsec virtual private networks (VPNs), and varying approaches to managing a private global backbone, including cloud-to-cloud peering. Ideally IoT traffic should not be sent via the public internet.

At the transport layer, the most interesting latest development is the IoT SIM Applet For secure End-to-end communication (IoT SAFE), developed by **GSMA** to allow for the use of the SIM card as a standardised hardware 'Root of Trust' for managing authentication between IoT devices and, typically, cloud servers. It provides mutual authentication between the end points and applies transport layer security (TLS) to the end-to-end communications.

### Cloud/data

This section applies equally whether the data is stored in the cloud or on-premises. Data storage considerations include protection from unauthorised access, modification or disclosure, the application of encryption, access controls and data back-up/recovery plans. As noted above, many cloud providers have specific requirements for security, in terms of protocols to be used for data transport. Other aspects of cloud security relevant for IoT include credentials, provisioning, access control, and device SDKs. Many cloud providers have a set of robust security-related tools for anomaly detection. Other issues for consideration at this layer include lack of security in interfaces and application programme interfaces (APIs), and data breaches.

### Application

Many security vulnerabilities derive from how applications are built. Often considerations for security will be low on the list of priorities. The key is to ensure that application developers are aware of security requirements and build the application in a way consistent with the security capabilities at lower layers. The application itself will handle authentication of users and data privacy.

### End-to-End

The concept of end-to-end security includes four main elements. First how the IoT application is built, considering all the security elements as a whole, such as using 'secure by design' principles, or having a consistent approach to update management. The second is to incorporate and integrate information from all layers to provide optimised security. This includes things like anomaly detection across device, network and transport layers. The third relates to ensuring that all the third party vendors have compliant security measures. The fourth is to have appropriate incident response capabilities, establishing procedures for identifying, containing, and removing cyber threats, and communicating with stakeholders, including law enforcement.

## Key considerations for enterprises in IoT security: framework and functions

As discussed in the sections above, there are growing security threats in IoT. Enterprises must be thinking both strategically about the best framework to establish in order to address security, and at the same time have one eye on the specific tools to be used.

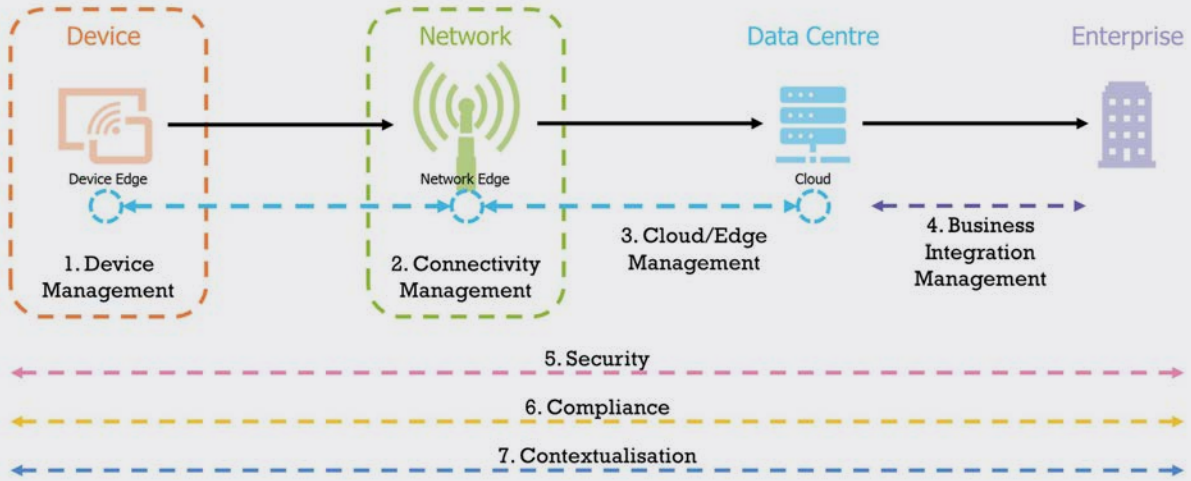
## Framework

An IoT Security framework should cover the following:

- **Dimension the problem**. Enterprises need an audit of devices, vulnerability assessment, penetration testing, and cyberattack simulations, to understand the security challenges and to have a rigorous approach to addressing them.
- **Understand your capacity for risk**. The appropriate level of security will always be dictated by a company's circumstances and its willingness to trade-off other factors (such as price or ease-of-use) in order to increase security. There is such a thing as too much security. ▶

**Figure 6:**
**The 7 Service Domains of IoT**

Source: Transforma Insights, 2022




- **Secure end-to-end**. The Internet of Things comprises a lot of different domains, any of which could be the weak point.
- **Secure by design**. End-to-end security should be considered during the process of developing the IoT solution, not overlaid at the end.
- **Establish policy and processes**. This might include things like network separation, strong passwords, use of public key infrastructure, and certificate management. It might also include compliance with standards, and consideration of ransomware insurance.
- **Compliance**. Establish a mechanism for ensuring that you are compliant with the ever-changing regulations relating to IoT and particularly security.
- **Train your people and partners**. The biggest security risk is generally the failure to follow established practices, which can be mitigated by training, including business certification such as ISO and Cyber Essentials.
- **Manage your partners**. You will almost invariably rely on third-parties for the provision of parts of your IoT project. You must also be confident that they are complying with best practice for security. Do your due diligence on them and their security practices.

## Functions

In parallel with the framework strategic considerations are the specifics of the IoT security features which should be implemented. The below are some of the most obvious mechanisms for mitigating security risks and should almost invariably feature as part of the considerations for securing an IoT deployment:

- Harden your devices to remove the risk of physical security breaches.
- Ensure that your devices can handle the necessary FOTA updates.
- Use features such as private APNs, IoT SAFE, and IPsec VPNs for robust network and transport layer security.
- Ensure continuous management of authentication and authorisation, for instance using hardware root of trust and digital certificates.
- Implement anomaly detection across all aspects of the IoT deployment, incorporating device, network and cloud.
- Apply automatic responses to security threats, for instance quarantining devices by blocking or constraining them.
- Remediation. And it needs to deal with breaches when they inevitably do happen.

Across these two areas of Framework and Functions there is a common aim: minimising the risk from IoT security risks, through establishing robust mechanisms for mitigating risk, reacting to breaches, and remediating.
IoT Security-as-a-Service

The complexity of building IoT solutions and the general lack of skills amongst most enterprises to span the entirety of the diverse elements of an IoT solution, mean that it is inevitable that IoT will be delivered predominantly as a managed service, rather than a stand-alone platform or product. Enterprises deploying IoT need trusted partners for the various elements. As part of its ongoing research on the evolving IoT landscape, Transforma Insights has identified a set of seven 'Service Domains' that will define how IoT is delivered . One of these domains is Security.

As outlined in the sections above, IoT security is a multifaceted and constantly evolving technology area. Few enterprises can be completely confident in their ability to stay on top of all of the constituent parts across end point, network and transport security, cloud/data security, solution design, anomaly detection, policy management, incident response and the other areas noted above.

The solution is to look for partners (and it's unlikely that a single partner will necessarily be able to cover every aspect) that can provide the IoT Security-as-a-Service function that will help to minimise an enterprise's risks.

## Digital Transformation


### About Transforma Insights

Transforma Insights is a technology industry analyst firm focused on the impact of emerging technologies and the associated technical and commercial best practice.

We help technology adopters understand the opportunities associated with new technologies, particularly the Internet of Things, but also in Artificial Intelligence, Distributed Ledger, Edge Computing and others under the umbrella of 'Digital Transformation'.

We help technology vendors understand the changing market dynamics and the associated market opportunity.

**www.transformainsights.com**

### Wireless Logic – IoT connectivity for any device, anywhere

Wireless Logic is a leading global IoT connectivity platform provider that simplifies and automates IoT management for any device, anywhere. With more than 10 million IoT subscriptions active in 165 countries and direct partnerships with 50 mobile networks, Wireless Logic provides reach into more than 750 networks across the globe and delivers value throughout the IoT connectivity chain.

Its purpose-built platform offers a single window to securely connect and manage assets across any network and number of deployments. For customers, this serves to simplify supply chains, accelerate time to market, lower the total cost of ownership and deliver connectivity that just works.

As an entirely customer and market-driven organisation, Wireless Logic meets its 25,000+ customers where they are to help them innovate by providing industry expertise, service support and the most flexible, resilient and secure connectivity solutions in the market. Its broad sector expertise includes industry, agriculture, healthcare, security, transport, utilities and smart cities.

**www.wirelesslogic.com**

# Will as-a-service offerings address the complexities of secure IoT?

The concept of IoT security-as-a-service has been formulated as a means for vendors of various secure IoT technologies to sell offerings to IoT organisations and thereby take away some of the security challenges they face. IoT organisations look likely to welcome the security-as-a-service approach if it can enable them to comply with new laws and protect their customers. But can a 'service' really enable this, asks George Malim

Security is focused on mitigating risks. If a system, technology or service can reduce the risk an organisation faces, it is worthwhile but the cost of the service must not outstrip either the value of the damage it protects against or the revenue the offering it is protecting generates. Simply put, sometimes security is too expensive for an IoT application to afford and this is why innovation is being brought to bear to automate, achieve economies of scale and eliminate reinvention of the wheel. IoT security-as-a-service initiatives are at the heart of this momentum but is a service what's needed to secure IoT?

"Every new option to secure IoT should be at the same time celebrated as a possible new alternative, but evaluated with care and within the limits of what it can provide," warns Daniel dos Santos, the head of Security Research at **Forescout**. "IoT security-as-a-service is one such alternative that can enhance the security of IoT deployments in organisations but at the same time, IoT is so diverse that often organisations need specific security policies that are difficult to deliver as a service. For instance, the security needs and related policies for Internet of Medical Things (IoMT) devices in a hospital will be very different from industrial IoT (IIoT) devices in a manufacturing plant and from enterprise IoT in a financial services organisation."

## Security is a spectrum

The idea of a service to secure IoT is therefore appealing if it is tied to the risk profile of an IoT offering and such a service looks set to become more appealing as volumes increase and the ▶

> ***"While the current IoT space is known to be fragmented, it's only going to become more so as companies continue to adopt and build out more functionality into future and existing systems"***

variety of IoT propositions on the market increases."IoT connected devices have become an integral part of daily life as more and more devices are attached to global networks," says Nathan Howe, the vice president of emerging technology at **Zscaler**. "For many organisations who find themselves in the race to adopt technology, implementing IoT-security-as-a-service has offered them a way to scale knowledge with speed and protection, at a fraction of the cost. And while some may argue that lowering costs can be detrimental to aiding future security, that's not always the case – in fact, it can very much depend on the organisation and its specific use cases."

"While the current IoT space is known to be fragmented, it's only going to become more so as companies continue to adopt and build out more functionality into future and existing systems," adds Howe. "Arguably most things in the future will come with some sort of sensor that can speak to networks, so we need to be prepared for the fragments to splinter even further. To ensure IoT devices are intelligent and protected with both current and future business requirements in mind, a suite of advanced security solutions needs to be installed as the system or service is being built. And regulations and legislations are helping in this regard – bringing more rigour to deployment strategies for new services as they go online. But they aren't affecting the billions of IoT services that are already online."

Iain Davidson, a senior product manager at **Wireless Logic**, sees the advantages of the as-a-service approach but warns that security must remain a multi-disciplinary landscape that involves multiple vendors. "The concept of IoT security-as-a-service is a good one, although it creates this idea that a single vendor can deliver all the component services," he confirms. "The cyber-attack surface of IoT is quite vast in some deployments, covering devices of different types from different vendors, networks, clouds, people and processes from your own organisation as well as suppliers, end-users and third party installers or maintenance staff. One provider cannot cover all the different security areas, but working with a lead vendor with a suitable framework and the ability to co-ordinate an ecosystem of partners can deliver the same outcome."

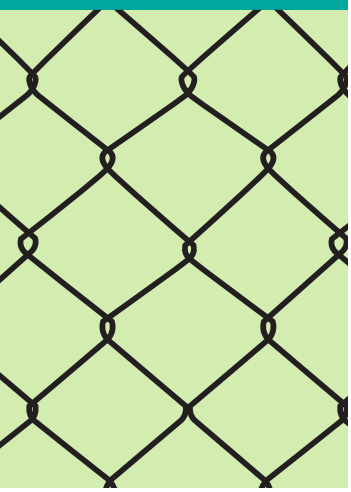
That collaboration is essential to provide reassurance to users of IoT services but it is also essential to address compliance concerns and corporate responsibility. "IoT security-as-a-service can certainly provide added reassurance that IoT deployments are protected, particularly when looking at the transmission of data between device and the cloud," says Camellia Chan, the chief executive and founder of **X-PHY**, a **Flexxon** brand. "However, this is only one aspect of a holistic cybersecurity approach. It's vital that businesses consider what exactly IoT security-as-a-service deployments entail and they don't simply shirk responsibility to providers offering seemingly watertight packages, which may only address very specific external layers."

"In fact, it is foolhardy to expect or claim 100% protection against cyber threats," she adds. "For ▶

**Camellia Chan**
**X-PHY**

**Iain Davidson**
**Wireless Logic**

***"Technically it could be realistic for organisations to go all in on as-a-service – but arguably from a responsibility, risk and governance perspective it isn't so we'll see a spectrum of responses,"***



any organisation, its data is its key asset and it should therefore be awarded multiple layers of protection, all the way down to the hardware level. Another way to think of it is, while you may close your garden gate, you'll still lock your house to provide the extra layer of security to your possessions."

For Howe, organisations are less likely to adopt security-as-a-service in isolation and they will instead take the approach for some aspects of their operations. The garden gate might be a service, while the front door lock could be managed internally.

"Technically it could be realistic for organisations to go all in on as-a-service – but arguably from a responsibility, risk and governance perspective it isn't so we'll see a spectrum of responses," Howe says. "The main question organisations should ask themselves when considering whether IoT security-as-a-service is right for them is whether they want to have control over their data. This can easily be determined by assessing how important data is to the company, or whether they're only reliant on it to deliver functions without knowledge. If it is important and if they are using it for knowledge versus just function that makes the argument for taking ownership of IoT security and managing their own risk over a third-party provider."

## Standards for non-standard scenarios

The emergence of IoT security-as-a-service is occurring at a time when frameworks and standards for securing IoT are starting to crystallise for the first time. This should allow IoT organisations to compare and contrast security offerings and to more accurately understand their obligations.

"The IoT security legislation and associated standards are long overdue and enterprise leaders are yet to make sense of them," warns Davidson. "While the legislators have focused on consumer applications, it makes sense for enterprise buyers to insist that the organisations they buy from, and the devices and solutions they procure, are compliant with best practices and have appropriate policies in place. That said, enterprises need to assess capacity for risk. The appropriate level of security might be dictated by customers, standards or perhaps by an assessment of acceptable risk and a trade-off between other factors such as price, compute resource or ease-of-use. The economics are really important here. Therefore, we should really be encouraging customers to think about the degree of risk and comply appropriately."

dos Santos also sees the push to standards but sees a long journey ahead. "There is an international push towards more stringent regulation regarding the development of IoT and connected devices and their use on organisations' networks," he says. "However, much of the discussion is still about making device manufacturers more responsible for the security issues on their products, including the presence of vulnerabilities and insecure default configurations such as hardcoded credentials. That is a valid, timely and important discussion, but organisations deploying and using those products are often left only with guidelines about secure configuration of devices and sometimes requirements about reporting security incidents involving those devices."

"Ideally, the organisations using IoT should share the responsibility for security with device manufacturers," he adds. "It is impossible to secure IoT by looking only at one end of the problem - either the manufacturers or the users - both need to act together to ensure a secure lifecycle for IoT devices. It took years to reach the current situation of seriously discussing and enacting legislation making device manufacturers responsible for the cybersecurity of their products and it will probably take a few more years before we see the same level of requirements for organisations using those devices."

IoT is so fragmented, operating across endpoints, clouds and networks that the threat surface is enormous and multi-disciplinary in nature.

**Nathan Howe**
**Zscaler**

**Daniel dos Santos**
**Forescout**

Innovations are often touted as the solution to IoT security but it seems fairer to say a portfolio of security solutions is required to deliver secure connectivity, trusted device identity and a host of cybercrime prevention tools and methods.

"To fully address these risks, it's crucial for organisations looking to implement IoT security-as-a-service to either only consider providers who can provide multi-layered data security down to the hardware level, or shore up their own defences in tandem by adopting their own hardware-based cybersecurity solutions to complement external defences," confirms Chan. "By doing so, they can close the loop when working with a vast conglomeration of connected devices, ensuring any threat that gets through the outer layers is thwarted at the point where data is at risk. Many IoT security-as-a-service offerings may claim universal protection across devices, but the evolution of threats means there's little surety in such services being bulletproof. Ultimately, data should always be protected from the hardware up to provide added security."

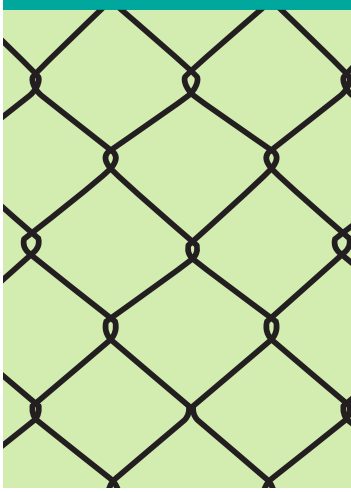
For dos Santos it's unrealistic to expect a single vendor to cover all the bases. "It is absolutely fair to say that a portfolio of solutions is required to secure IoT," he agrees. "IoT devices go through a lifecycle of design, development, production, utilisation, support and retirement. In each of these phases there are technologies and processes to ensure security, such as secure development for device manufacturers and zero trust network architectures for device users. IoT devices also often use a combination of technologies such as cloud backends, wireless networks and a multitude of sensors and actuators. It is unrealistic to expect that a single technology can solve all the problems in every phase of the lifecycle for every component of every device. Another important point is that even if a device is designed, developed, configured and used securely according to today's standards, it may not be secure tomorrow, since threat actors are always evolving and the threat landscape is changing. A simple example is the use of encryption algorithms which are considered safe for some time until a flaw is discovered."

Given this, is the as-a-service approach a stronger way to accommodate the continuous changes that characterise IoT security? dos Santos sees the value and the potential weaknesses of the approach. "Most likely not every security solution can be provided as-a-service," he agrees. "There are parts of the IoT device lifecycle that are inherently the responsibility of specific players. It is unrealistic to expect that a service can make every IoT device in every organisation secure the same way."

"For instance, which devices should be allowed to communicate to which other devices and what to do when an attack is detected are examples of decisions that are individual to each business organisation," he adds. "**Colonial Pipeline**, when facing a ransomware attack, chose to bring their OT systems offline to prevent further spread, but not every organisation would take the same decision, so this type of decision cannot be provided as a service that fits every need. Risk is necessarily shared across all involved parties. When a company provides a service to another company, the user of the service faces the risk that the service provider will be breached and sensitive data exfiltrated, as was the case with remotely managed **Verkada** IP cameras in 2021 or, worse, that the service provider can be a point of entry into other organisations, as was the case with **Kaseya** VSA, also in 2021."

For Davidson, it's clear that a service can meet more of the market's needs most but not all of the time. "The term IoT security-as-a-service is a good as it encourages enterprises to look to partners and best practices to help them," he says. "Not all enterprises will have the experience in-house, they should turn to partners for advice or to assist with implementation. The as-a-service term could be an over-reach if it were to be interpreted as removing risk altogether as opposed to mitigating risk and managing the impact of security breaches."

***"Ideally, the organisations using IoT should share the responsibility for security with device manufacturers"***



# How to **Measure IoT Success?**

beecham research

Shaping the IoT future

IoT is increasingly important to business operations. As a result, improving the success rate of IoT projects is now crucial.

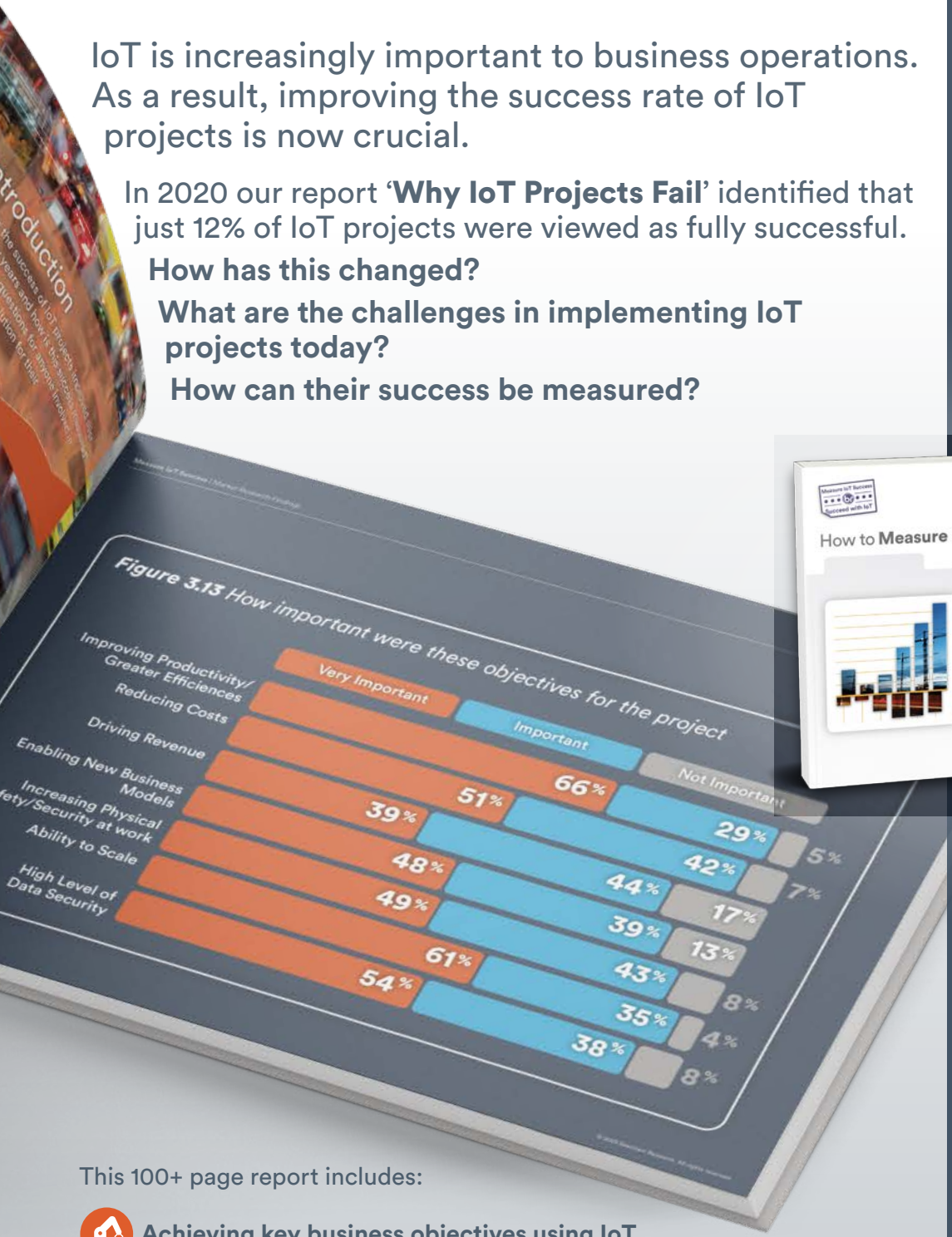
In 2020 our report '**Why IoT Projects Fail**' identified that just 12% of IoT projects were viewed as fully successful.

**How has this changed?**

**What are the challenges in implementing IoT projects today?**

**How can their success be measured?**

This independent analyst report is the latest addition to Beecham Research's popular 'Succeed with IoT' series.





Report sponsored by...

Airgain

KORE

MULTITECH

software AG

THALES

This 100+ page report includes:

- Achieving key business objectives using IoT
- Exclusive interviews with senior executives in the IoT market
- Research findings from 4 recent user surveys
- Compared with our research findings from 2020 – what's changed?
- Insights on our research findings from leading IoT market players
- Case studies on measuring IoT success

**Dowload for FREE at: www.measureiotsuccess.com**

# Can GSMA's new framework secure cellular IoT?

beecham research

SPONSORED BY

THALES

Building a future we can all trust

# The likelihood of an IoT security breach is increasing and so is the cost

## This report, by Robin Duke-Woolley, the chief executive of Beecham Research, outlines the IoT security framework for cellular devices being established by GSMA, working with key industry stakeholders

As IoT solutions become increasingly important to business operations, the cybersecurity threat level is also increasing. Compared with a few years ago, IoT solutions are becoming:

- **Larger** Deployments of 10,000+ connected devices are becoming more common as IoT moves towards massive IoT
- **Critical** Immediate, low latency trustful data for automation and control is required
- **Extended** Coverage over large geographic distances, including worldwide is needed
- **Interoperable** The ability to work with a wide range of other systems has become essential
- **Complex** More is being done remotely, and all of this must be maintained – remotely

Each of these increases the impact of cybersecurity issues, and the threat level is therefore increasing over time. It is now a question of when there will be a security breach for an IoT business user, not if, and minimising the severity of that.

The cost of a security breach comes primarily in three parts – operational, reputational and repair. The operational cost is usually measured in terms of the cost of downtime, which for a factory or other automated plant could be substantial. The reputational cost is potentially much higher, particularly for a well-known brand. To these must be added the cost of repair – it may be necessary to replace everything that has been deployed because the breach cannot be repaired remotely. As a total cost of ownership, these could represent a huge cost when combined together. ▶

**Robin Duke-Woolley**
**Beecham Research**

With the increasing likelihood of a security breach in mind, and the potential cost of that, how can enterprises ensure the effectiveness of their IoT security solution remains at the highest level over time?

Related to this, IoT security is a complex topic. Suppliers may claim their IoT security solution is secure and meets all these threats now and in the future. But can they prove it?

## Establishing the proof

Such proof can be provided by a certification process, where the process is operated by a recognised independent third party using a scheme endorsed by the industry at large. Recognised in this case must mean recognised by the industry as an expert in security, with no vested interest in supply. Such a scheme is measurable, repeatable and objective, and as a result creates trust.

What should be certified? The secure hardware and secure software components that form the basis of the security solution.

Is it necessary to have both secure hardware and secure software components? Yes. Secure software on its own can always be hacked. If that structure can be changed, it can be cloned, impersonated or interfered with in many different ways. Secure hardware, on the other hand, is much more difficult. This is because hardware security means burning secure identifiers/secure credentials into the hardware, which cannot then be physically tampered with nor extracted. That is how the highest level of security can be created. It is called a secure Root of Trust and considerably more secure than anything else.
It is then a question of the level of security needed. If a low level of security is acceptable – for example, perhaps for a headset – then a pure software solution may be sufficient. How important is it not to be exposed to attack, even remotely? If there is less security, the risks are higher, which means that a balance must be struck – with full knowledge of the risks.

Does that add unnecessary extra cost? It need not be expensive, but compared with the cost of a breach as outlined earlier it is likely to be tiny anyway.

## A mobile framework

The mobile industry has a particular interest in ensuring the highest levels of security because so much of our world is going mobile. According to **GSMA**, there are around 5.5 billion mobile device users around the world, plus nearly three billion cellular IoT connections, and the way consumers use their devices is evolving. With consumers increasingly relying on digital services across all aspects of their lives, the telecoms industry is facing rising demand for applications running on mobile devices like payments, transport ticketing, identity management and secure IoT services:

As the Trusted Connectivity Alliance (TCA) makes clear "Given the sensitivity of these applications, their critical role and the data they contain and share, it is crucial that the mobile telecoms industry has the appropriate security mechanisms to protect users and enable the market to reach its full potential. In response, the industry is leveraging the advanced capabilities of proven technologies already available in mobile devices that enable trusted cellular connectivity – such as eSIM – to provide the requisite security for these applications. This approach reflects the growing momentum for eSIM technology." ▶

### 1. Payment

The COVID-19 pandemic has accelerated the adoption of digital payments, with mobile devices enabling touchless methods such as EMV® contactless and QR codes. These are set to be 4.4 billion mobile wallet users by 2024 and the global mobile payment market is predicted to grow annually by 23.7% between 2021-26. (Source Juniper Research) This will see the value of digital wallet transactions reach $12 trillion - up from £$7.5 trillion in 2022. (source: iMARC)

### 4. Transport Ticketing

The days of relying on paper tickets are over as many public transit authorities are now offering passengers increased convenience, flexibility and security through mobile ticketing, where travellers can order, buy and validate tickets with their smartphone or wearable device

### 3. Mobile Identity

As mobile devices become the primary point through which consumers interact with service providers, the ability to securely identify and authenticate end-users is increasingly critical. Consequently, enabling users to authenticate themselves through their device for a varity of use cases - including banking, payments, government services and healthcare - promises significant benefits. In addition, mobile devices are increasingly used in place of physical identity documents, such as e-passports and mobile licenses (mDLs).

### 4. Secure IoT Services

The increasing number of high-end connected consumer IoT devices is driving demand for various secure services that can protect IoT data communications from the IoT device to the cloud.

**Figure 1: Secured applications offer great potential**

Source: Trusted Connectivity Alliance Ltd (TCA) – Realising the Potential of Secured Applications for Mobile (SAM), February 2023

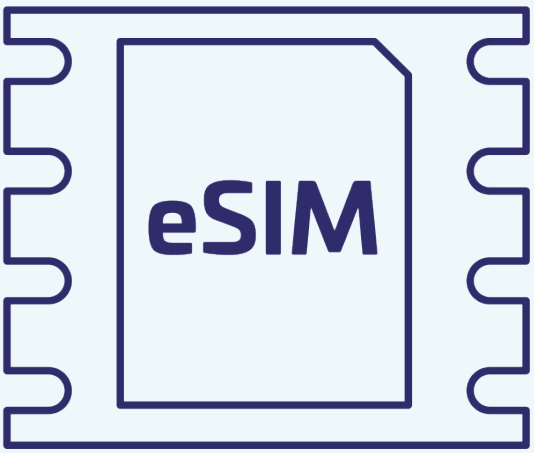
In response to these trends, it makes sense to have one overall framework to cater for all of these digital services – one that all suppliers in each of these areas can work with and inter-operate in. A standard approach for the whole mobile industry, which in turn reduces unit costs.

It is with this in mind that the GSMA together with mobile network operators (MNOs) and the supply industry including Thales has created a framework, comprising the following parts. Note that eSIM in this report means standalone or integrated eSIM (often referred to as iSIM):

1. eSIM architecture and technical specifications, including remote SIM provisioning (RSP)
2. An update on the RSP specification for provisioning constrained devices (low power, low data rate) to enable massive IoT – SGP .31/32
3. embedded universal integrated circuit card (eUICC) secure assurance (eSA) – the certification process for secure eSIM devices
4. IoT SIM Applet For Secure End-2-End Communication (IoT SAFE) – secure IoT services based on the eSIM
5. Secured applications for mobile (SAM) – extending the eSIM/iSIM to cover other digital services for mobiles where high-level security is essential

These all relate to the eSIM as a basis for IoT security for connected devices. In addition, but not directly part of the security solution for the devices, is the security accreditation scheme (SAS) for suppliers.

**Thales** occupies a unique position in the field of eSIM solutions. The company's solutions have been adopted by large numbers of original equipment manufacturers ▶




(OEMs), telecoms operators and key industry players worldwide. It has ongoing business relationships with 450 MNOs and over 100 OEMs in the IoT/M2M and consumer markets. Responsible for more than 360 projects, Thales is the world leader for RSP platforms, employed in both consumer and IoT/M2M environments.

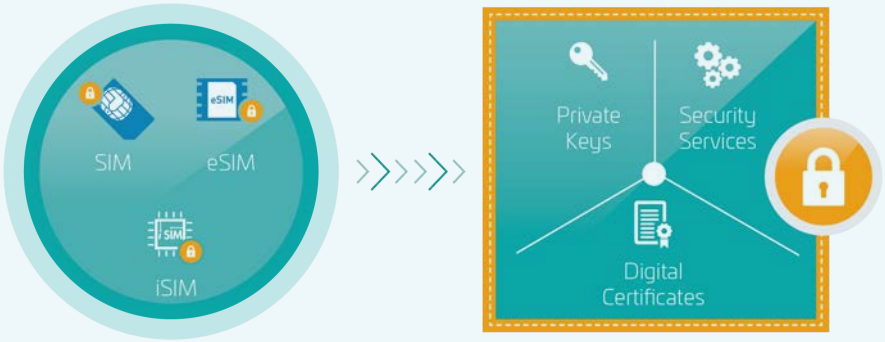
As part of that, Thales is actively and directly involved in the creation of these and new specifications, collaborating with the GSMA and other key stakeholders to establish an interoperable security framework.

## Building the IoT Root of Trust

In order to ensure data security, the element of trust is paramount. Connected IoT devices are playing an increasingly significant role in every industry sector – from transport infrastructure and autonomous vehicles, through to greater automation in manufacturing operations, smart energy and faster diagnosis and treatment in healthcare. The core of all of these advances is the huge amounts of data they generate and, as greater reliance is put on that data for increasingly mission-critical activities, that data must be trusted. To be trusted, it must be recognised as coming from the right source, at the right time, in the right format and in no way corrupted.

Trust is essential to realise the full potential of the IoT. Digital security must be designed into IoT devices from the ground up and at all points in the solution to prevent vulnerabilities in one part from jeopardising the security of the whole. This is easy to say but IoT solutions can be complex and are becoming more so over time. Machines and objects in virtually any industry can be connected and configured to send data over cellular networks to cloud applications and backends. The digital security risk is present at every step along the IoT journey, and there are growing numbers of hackers at national and international levels that seek to take advantage of a system's vulnerability.

Risk must be mitigated for the entire IoT lifecycle of the deployment, especially as it scales and expands geographically. That requirement is provided by the Root of Trust (RoT), which is a set of implicitly trusted functions that the rest of the system or devices can use to ensure security. In IoT the RoT consists of identity and cryptographic keys built into the hardware of a device. It establishes a unique, immutable and unclonable identity to authorize a device in the IoT network. Since the root key is generated internally and never exposed, no sensitive data is visible anywhere in the supply chain. It is a source that can always be trusted within a cryptographic system. Because cryptographic security is dependent on keys to encrypt and decrypt data and perform functions such as generating digital signatures and verifying signatures, solutions will normally include a hardened hardware module – a tamper resistant element (TRE). A TRE is a microprocessor chip that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. Essentially, the security framework must fulfil three key requirements: ▶



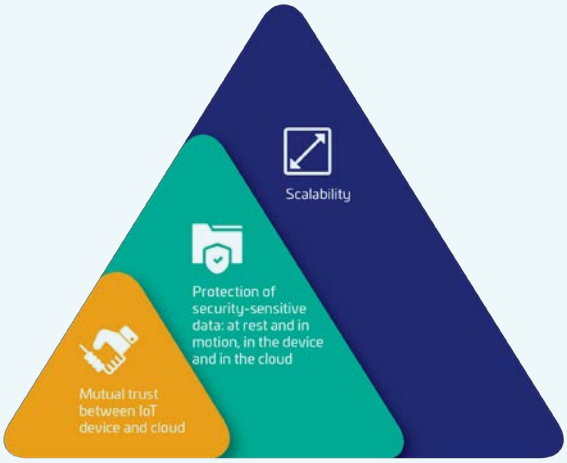

Hardware cryptographic toolbox

Inside a hardware cryptographic toolbox

1. *Mutual trust between IoT device and cloud*
- Authentication - Device applications and IoT cloud applications need to exchange security-sensitive data. Trust must be established between the two applications before any such exchange takes place.

2. *Protection of security-sensitive data: at rest and in motion, in the device and in the cloud*
Two factors must be addressed here:
- Integrity - ensuring that the data has not been modified
- Confidentiality - ensuring that data is never disclosed to an unauthorised party

3. *Scalability*
With an exponential increase in the number of connected devices already underway, any security framework for the IoT must be scalable.




## Why is the eSIM ideally suited to the demands of IoT security?

eSIMs can deliver scalable 'security by design' for IoT.

Thales' approach meets the scalability requirements of an IoT security framework by utilising standardised and field proven eSIM technology, irrespective of form factor, and building on experience from the billions of devices already deployed in the field. These tamper resistant elements are a standard technology that can integrate with the new GSMA specifications. Within this standardised framework, irrespective of their form factor, eSIM provides the same level of protection.

## How does the eSIM-based approach work?

The foundation of any secure process is the handshake protocol between the IoT device and the cloud; mutual authentication must be enabled before any data exchange can occur. Specifically, this is achieved through hardware tamper resistant element-based security and cryptography, and GSMA specifications regarding:

- *The means by which the IoT device requests authentication from the cloud:*
device applications need to communicate in a language understood by the IoT security applications stored in eSIM to request authentication of the cloud. This language (which is the application programme interface (API) between the device middleware and the applet in the eSIM) is common to both device and hardware tamper resistant element, so therefore becomes scalable.

- *The means by which the cloud requests authentication from the IoT device:*
cloud applications need to communicate in a language understood by the IoT security applications (also in the cloud) to request authentication of the IoT device.

Once this handshake protocol is completed, the secure transport layer (TLS) is established, and can protect the data exchanged between the device and the cloud.

Within this framework, eSIMs are tamper resistant elements which can be regarded as cryptographic toolboxes serving two main purposes:

- Secure storage of security credentials
- Secure execution of security-sensitive services via IoT security applications

As a result, they address the three key IoT security requirements:

1. *Mutual trust between the IoT device and cloud*
- The device's private key, stored in the hardware tamper resistant element, is used to sign authentication data to the cloud
- The cloud digital certificate in the hardware tamper resistant element is used to authenticate the cloud
- This end-to-end mutual authentication enables a TLS connection

2. *Protection of data at rest and in motion*
- The device's key is stored safely in the hardware tamper resistant element ▶

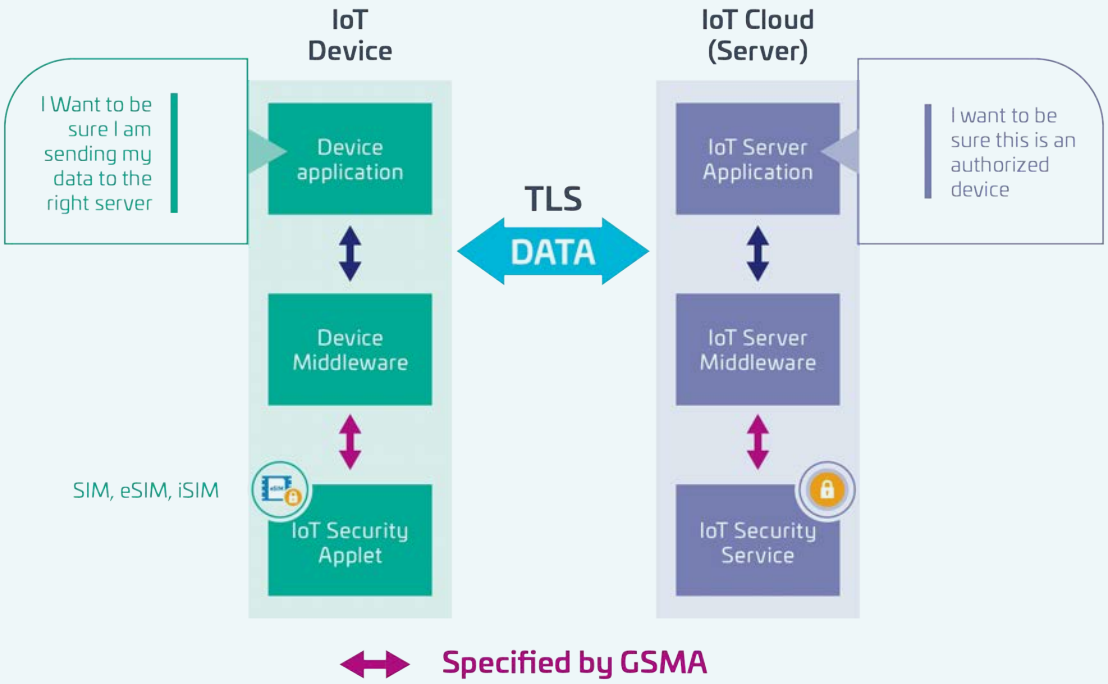



**Figure 2: Handshake protocol: Transport Layer Security**

- Onboard key generation capabilities
- Data is digitally signed by session keys calculated during the TLS handshake; the cloud can verify the integrity of the exchanged data
- The TLS ensures confidentiality between the device and the cloud

3. *Scalability*
- There are already billions of hardware tamper resistant elements in the field

Furthermore, all these security services pave the way for further services, including verification of IoT device firmware and remote lifecycle management of IoT security devices in the field, such as renewal and revocation of keys.

Keys are in the hardware tamper resistant element (device keys and cloud certificate) and the IoT Server Middleware (cloud keys and device certificate).
The IoT Security Server's role here is to provision the hardware tamper resistant element and the cloud and to manage the life cycle of the credentials.

## eUICC Secure Assurance (eSA)

The purpose of GSMA eUICC Security Assurance (eSA) scheme is to provide a certification process for eUICC manufacturers of their secure hardware and software associated with eSIM/iSIM technology, for the purpose of demonstrating resilience against a range of high-level attack threats.

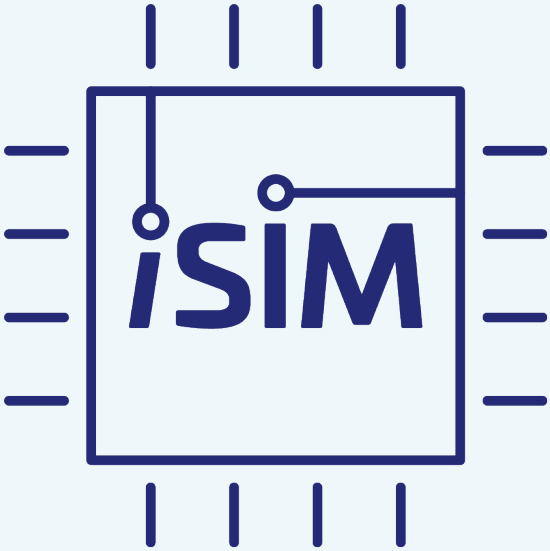
This certification is conducted by an independent third party, typically a laboratory recognised by the industry as an expert in cybersecurity and endorsed by the GSMA. It is not sufficient for a supplier to self-certify. With the best will in the world, that way leads to mistakes being made. There must be an external examiner for something so critical. Such a scheme is then measurable, repeatable and objective, and as a result can create trust. The methodology used is itself endorsed by industry, using criteria that are common not proprietary.

The scheme is designed to expedite the eUICC security certification process, overcome complexities, and reduce time to market for eSIM products. The scheme requires manufacturers to prove a benchmark level of security resilience across product processes. It does this by combining high-security quality with a pragmatic evaluation implementation approach adapted for the mobile market. The processes are in line with industry and ISO requirements and reflect the highest common criteria security standards recognised in Europe. While based on the common criteria approach to security assurance, it is more condensed, making the process fast and efficient. As a result, it represents a faster way to market than the alternative routes.

This demonstrates a very secure platform that can then be used to build secure services on top, such as IoT SAFE.

## GSMA IoT SAFE

The standardised eSIM specification was developed by the GSMA as a response to the problems of using the traditional plastic SIM cards in IoT devices. A further GSMA initiative is IoT SAFE. This recommends that the industry should use the SIM as a hardware TRE or Root of Trust to achieve end-to-end, chip-to-cloud security for IoT ▶




products and services. It is widely accepted technically that the SIM is particularly well-suited for this purpose: it is one of the hardest of all identifiers to spoof, with advanced security and cryptographic features, is fully standardised, and has been deployed in huge numbers of devices for the past 30 years. Key characteristics of IoT SAFE include:

- Use of the SIM/eSIM as a mini 'crypto-safe' inside the device to securely establish a TLS session with a corresponding application cloud/server
- Compatible with all SIM form factors such as eSIM and more recently iSIM. eSIM/iSIM are particularly suitable for IoT SAFE since they are certified as per eSA
- Provides a common API for the highly secure SIM to be used as a hardware Root of Trust by IoT devices
- Helps solve the challenge of provisioning millions of IoT devices

The IoT SAFE applet runs on Java virtual machine, which in turn runs on the eSIM OS. In implementing this GSMA initiative, the Thales approach meets the scalability requirements of an IoT security framework by utilising standardised and field proven eSIM/iSIM technology, irrespective of form factor, and leveraging the billions of devices already deployed in the field. The company is actively and directly involved in the creation of new specifications, collaborating with the GSMA and other key stakeholders to establish an interoperable security framework. Indeed, tamper resistant elements are a standard technology that can integrate with the new GSMA specifications.

Thales has not only implemented the new GSMA IoT SAFE specifications. IoT SAFE is standard but there is additional value that can be provided to customers. The company works with providers of security stacks, TLS structures for example, to make sure the integration is easy. Touchless provisioning is also provided – a way to totally remove the cost impact of adding security into a device when the device is manufactured. When using Thales' IoT SAFE in the device, there is no change to the manufacturing process because the device credentials will be generated on board the device when it is deployed. There is no additional activity and no additional charge in the process because the touchless provisioning system works together with the security that Thales provides.

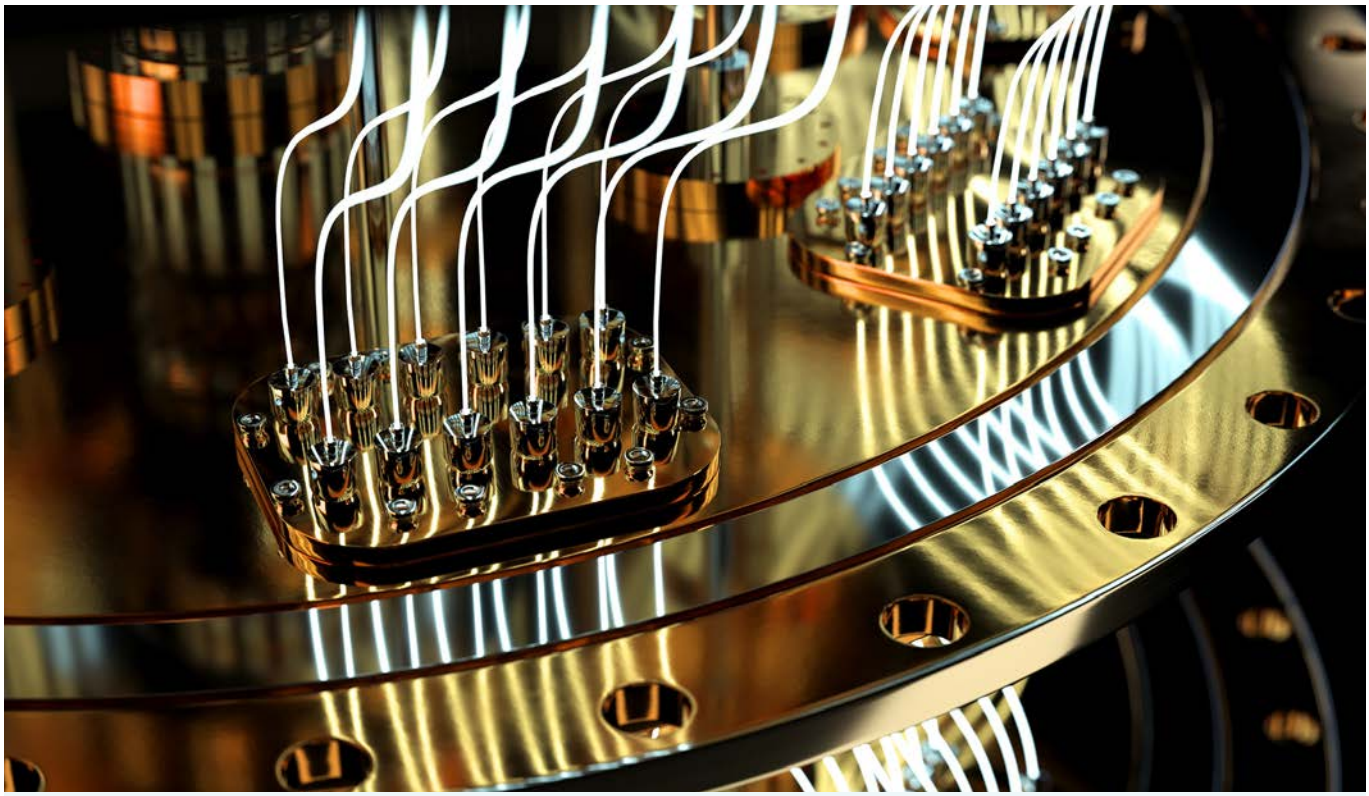
## Secured applications for mobile (SAM)

As noted earlier in this paper, with consumers increasingly relying on digital services across all aspects of their lives, the telecoms industry is facing rising demand for applications running on devices like payments, transport ticketing, identity management and secure IoT services.

In response, the industry is leveraging the advanced capabilities of proven technologies already available in mobile devices that enable trusted cellular connectivity – such as eSIM – to provide the requisite security for these applications. This approach reflects the growing momentum for eSIM technology.

With these trends in mind, it makes sense to have one overall framework to cater for all of these digital services – one that all suppliers in each of these areas can work with and interoperate in. A standard approach for the whole mobile industry, which in turn reduces unit costs.

To support this trend for utilising the eSIM to host secure applets, GSMA published Secured Applications for Mobile – Requirements Version 1.0 [SAM.01] in June 2021. By providing a secure domain within the eSIM that enables access to applications regardless of the operator profile used, it is considered that this initiative presents significant opportunities to support new use-cases through proven, secure and reliable hardware technology. This goes beyond SIM functionality and provides a way to decouple the application layer security from the connection to the mobile network itself. Such functionality can then become 'transversal', where secure services like IoT SAFE can sit and be executed in a secure manner but independent from the connectivity providers. ▶



## EU Cybersecurity Act

A further consideration is the EU Cybersecurity Act, which was passed in June 2019.

The EU Cybersecurity Act is a law that gives more authority and resources to the EU Agency for Cybersecurity, formerly known as ENISA. It also creates an EU-wide cybersecurity certification framework for ICT products, services, and processes. The framework will consist of common cybersecurity requirements and evaluation criteria across national markets and sectors. The certification will be recognised in all EU Member States and will be voluntary at first, but may become mandatory for critical products or activities. The EU Cybersecurity Act is part of the Digital Single Market initiative, which aims to increase data security and harmonize the rules for the digital economy in the EU. The EU Cybersecurity Act is still in the early stages of development and will affect the international standards community.

## Security accreditation scheme (SAS)

Although beyond the scope of this paper to include in any depth, it is worth noting that the GSMA's security accreditation scheme (SAS) is a further part of the overall eSIM framework. This enables mobile operators, regardless of their resources or experience, to assess the security of their eSIM suppliers, and of their eSIM subscription management service providers.

## Looking to the future

New cybersecurity threats are constantly emerging and new ways of dealing with them will be required. One such is post quantum cryptography (PQC), cryptographic algorithms that are thought to be secure against a cryptanalytic attack by a quantum computer. Thales is working on these new algorithms to combat such threats as they relate to SIM products. The company is investing heavily in security technologies – spending money researching new threats to make sure that future technologies are sufficiently secure for businesses to use effectively.

There is no doubt that IoT security is complex, and this will become more so over time. IoT users have a choice. They can have their own expert security team, maintain these skills, keep up to date with new threats arising and invest accordingly. Alternatively, they can work together with a security expert like Thales to assist in minimising both the cost and time to market. ■

### About Thales

Thales (Euronext Paris: HO) is a global leader in advanced technologies within three domains: Defence & Security, Aeronautics & Space, and Digital Identity & Security. It develops products and solutions that help make the world safer, greener and more inclusive.

The Group invests close to €4 billion a year in Research & Development, particularly in key areas such as quantum technologies, Far Edge computing, 6G and cybersecurity.

Thales has 77,000 employees in 68 countries. In 2022, the Group generated sales of €17.6 billion.

THALES
Building a future we can all trust

**Further reading:**

**GSMA IoT SAFE**

**Thales Adaptive Connect**

**Massive IoT: Tech overview, business opportunities and examples**

# The winners of the 2023 IoT Global Awards are...

It's officially the time of year when WeKnow Media announces the winners of its 2023 IoT Global Awards! This prestigious awards programme recognises innovative firms, products, and talent from across 11 Internet of Things (IoT) industry categories. After receiving hundreds of applications from the very best corporations, companies, start-ups and industry leaders, the winners have been chosen

The 2023 IoT Global Awards, an industry benchmark for excellence in IoT, provided organisations with an opportunity to demonstrate their most innovative IoT technologies or apps that are most valuable or advantageous to users and providers, with the larger goal of promoting IoT. The winners have been chosen by an independent and qualified panel of judges consisting of industry and subject matter experts, analysts, directors, CEOs and academics.

Leading the Awards team, WKM's head of Digital Services, Maciej Szelezin said that it's truly inspiring to witness the exponential growth of the IoT Global Awards year after year. "As an avid follower, I couldn't be more delighted to see the increasing number of participants and the breadth of innovative solutions they bring to the table. Recognising and celebrating outstanding achievements within this rapidly evolving field is crucial in driving innovation and progress. It's ▶

# Here are the Winners of the 2023 IoT Global Awards:

## Category Company

**Automotive, Transport & Travel:**
Overhaul

**Big Data, Cloud & Analytics:**
Avarisoft

**Connected Consumer & Smart Home:**
Ci Smart Fire Prevention Technology

**Connected Health Or Wearable Tech:**
Monnit

**Industry & Construction:**
fischerwerke

**Research & Development Or New Launch:**
Pod Group

**Retail, Marketing & Hospitality:**
Uber Technologies

**Securing IoT:**
Atsign

**Smart Cities, Government & Utilities:**
Connectpoint

**CxO of the Year:**
Nick Earle of Eseye

**Start-Up, Business Development Or Ecosystem Of The Year:**
iBASIS

**Nick Earle**
Eseye

***"This award is a testament to the amazing team at Eseye who work tirelessly to drive innovative IoT connectivity solutions for our customers"***

heartening to see so many talented individuals and organisations contributing to this global effort. Congratulations to all the entrants, and here's to another successful year of pushing the boundaries of what's possible in IoT."

Nick Earle, this year's CxO of the year, has taken his extensive business and tech experience and used it to analyse connected business challenges and opportunities for IoT-enabled business disruption. Under his leadership, **Eseye** has delivered benefits across industries, enabling water supply to remote African villages, and providing a new range of managed services for smart meter users, while also personalising customer experience for vending machine users.

"I'm humbled to accept the award of IoT CxO of the Year," Earle said. "This award is a testament to the amazing team at Eseye who work tirelessly to drive innovative IoT connectivity solutions for our customers," he added.

Addressing the challenges and drawbacks of being a corporate leader in the IoT industry, Earle pointed out that "the fundamental problem with IoT is that although we have known for 15 plus years its potential to deliver new forms of value, it is still too complicated for most people to implement. This is because there are hundreds of component solutions most of which were not designed to work with everything else."

At Eseye, "we bring together all the mobile network operators - over 800 - and all the communication technologies into one solution for any IoT device," Earle explained. "We also insist on analysing and optimising the firmware of our customers' devices before we start work. ▶

Monnit's work with babies in sub-Saharan Africa impressed the judges

Uber Technologies were recognised for the UberSIM


This can mean that our sales cycles are much longer as we are trying to solve a bigger problem. But ultimately it delivers more value to customers," he added.

**Uber Technologies**' UberSIM project was recognised in the 'Retail, Marketing and Hospitality' category this year. The UberSIM initiative is a significant step towards simplifying global IoT mobile connectivity, with a clear focus on scaling economically.

"The UberSIM team is extremely honoured to have won the 2023 IoT global award for Retail, Marketing and Hospitality sector," Aseem Ghai, the associate manager of technical supply chain and operations for IoT & Wireless at Uber, said. "Receiving the award at the world's biggest IoT stage proves we are doing something right and inspires us to take the next step in extending the capabilities of UberSIM to Uber riders, drivers, couriers, eaters and restaurants."

Explaining what led to the development of UberSIM, Ghai said that Uber works with multiple connectivity partners and various business use cases across the globe. "We wanted to have a single application programme interface (API) interface for our teams internally to manage and control the connectivity options in different regions. Thus, the IoT & Wireless Supply chain team at Uber developed an internal connectivity-as-a-service solution called UberSIM which is based on GSMA's embedded universal integrated circuit card (eUICC) standard."

UberSIM integrated global MNOs and MVNOs into the SIM, with API-based switching made possible, according to Ghai. "It also provided over-the-air (OTA) switching of carriers, multiple local carrier integrations, pay-as-you-go model, and a single pane of glass view into Uber's IoT and wireless landscape."

***"The UberSIM team is extremely honoured to have won the 2023 IoT global award for Retail, Marketing and Hospitality sector"***
**Aseem Ghai, Uber**

**Connectpoint**'s Falcon Text-To-Speech Device won in the 'Smart cities, government, and utilities' category for its innovative approach to IoT, user value and IoT advantages.

"Winning the 2023 IoT Global Awards validates the years of development work required to produce the first-of-its-kind solar text-to-speech device," Rick Wood, the president and CEO at Connectpoint, said. "The Falcon addresses a significant underserved group of individuals: the visually impaired. This product will provide the visually impaired with the same transit service information as those without visual impairment."

Addressing the challenges faced when implementing Falcon, Wood said that "because there is no electrical infrastructure at the majority of bus stops around the world, we need ▶

**Connectpoint has been helping travellers find their destinations**


**Nick Earle's mission to integrate and simplify IoT earned him CxO of the year**

to develop a solar-powered device that manages power very efficiently. The Falcon body is covered by solar panels. The energy created from the solar panels needs to be stored in very small batteries and these batteries need to power the printed circuit board (PCB) board and modem. Both of which require a significant amount of power to operate."

Confirming that Falcon is heading to international markets, Wood added that "Connectpoint absolutely plans to take the Falcon to the international market. It comes with a five-year warranty and can accommodate up to 80 languages."

**Monnit** received the award in the 'Connected health or wearable tech' category for its Save Sub-Saharan African Newborns with IoT project, which illustrates the collaborative ecosystem and role IoT technology can play in addressing global healthcare concerns.

"Winning the 2023 IoT Global Award in Connected Health or Wearable Tech is a great honour for our company," Brad Walters, founder and CEO at Monnit, said. "We consider it a gratifying culmination after many years of working with partners to bring unique solutions to the market. Through these projects and this award, we're inspired to continue improving many aspects of life - like better health care, facilities management, labs, factories, air and productivity in nearly any industry."

Looking into the challenges Monnit faced when it came to the implementation of its IoT technology in Africa and how they were overcome, Walters thinks that the biggest challenge in these unique IoT applications starts with truly understanding the issue that needs to be solved. "This helps us determine where and how Monnit can contribute to creating a customised solution," he added.

As a reward, each winner will get a digital badge that can be used for digital marketing materials to announce the win, plus a logo and company details will be displayed on the Winners page. On top of that, winners will receive full social media coverage and a video wrap-up clip with their logo and winning category.

***"Winning the 2023 IoT Global Award in Connected Health or Wearable Tech is a great honour for our company"***
**Brad Walters, Monnit**

While we have made every effort to ensure the accuracy of this listing, the pandemic means that many events are changing timing, dates and locations. Therefore please check at the events' websites to ensure details are up-to-date before travelling.

**IoT Tech Expo North America**
17-18 May 2023
Santa Clara, California, USA
**https://www.iot-now.com/event/iot-tech-expo-north-america-2/**

**Digital Transformation Week North America**
17-18 May 2023
Santa Clara, California, USA
**https://www.iot-now.com/event/digital-transformation-week-north-america-2/**

**Edge Computing Expo North America**
17-18 May 2023
Santa Clara, California, USA
**https://www.iot-now.com/event/edge-computing-expo-north-america-2/**

**The Battery Show 2023**
23-25 May 2023
Stuttgart, Germany
**https://www.iot-now.com/event/the-battery-show-2023/**

**IoT Visions Zurich**
15 June 2023
Zurich, Switzerland
**https://www.iot-now.com/event/iot-visions-zurich/**

**Sensors Converge**
20-22 June 2023
Santa Clara, California, USA
**https://www.iot-now.com/event/sensors-converge/**

**AI Hardware & Edge AI Summit**
20-22 June 2023
Santa Clara, California, USA
**https://www.iot-now.com/event/ai-hardware-edge-ai-summit/**

**The Things Conference 2023 Amsterdam**
21-22 September 2023
Amsterdam, The Netherlands
**https://www.iot-now.com/event/the-things-conference-2023-amsterdam/**

**IoT Tech Expo Europe**
26-27 September 2023
Amsterdam, The Netherlands
**https://www.iot-now.com/event/iot-tech-expo-europe-2/**

**Digital Transformation Week Europe**
26-27 September 2023
Amsterdam, The Netherlands
**https://www.iot-now.com/event/digital-transformation-week-europe-2/**

Kaleido Intelligence

# Enterprise Cellular IoT Demands & Opportunities

## Key survey results from 800 IoT professionals

Join us for our webinar on **May 24th at 3PM BST** to receive exciting insights from the world's most comprehensive survey on cellular IoT connectivity. Plus, receive an exclusive **free** whitepaper following the event!

**Join our expert panel**

**Steffen Sorrell**
Kaleido

**Gabriele Salvate**
BICS

**Sam Copsey**
Pod Group

**Loic Bonvarlet**
Kigen

**Niall Strachan**
Pelion

**To sign up visit:**
www.iot-now.com


# Stay Competitive in Today's Connected World

Leverage secure, reliable and robust wireless solutions to improve operational efficiencies, productivity and safety in industrial factory environments.

- ☑ Factory Automation
- ☑ Predictive Maintenance
- ☑ Robotics
- ☑ Asset Tracking

# Wireless Industrial Solutions


Wireless Modules


System-On-Modules


Sensors


Gateways

Bluetooth® WiFi™ LoRaWAN® LTE-M NB-IoT™

**Learn More:** www.lairdconnect.com/industrial