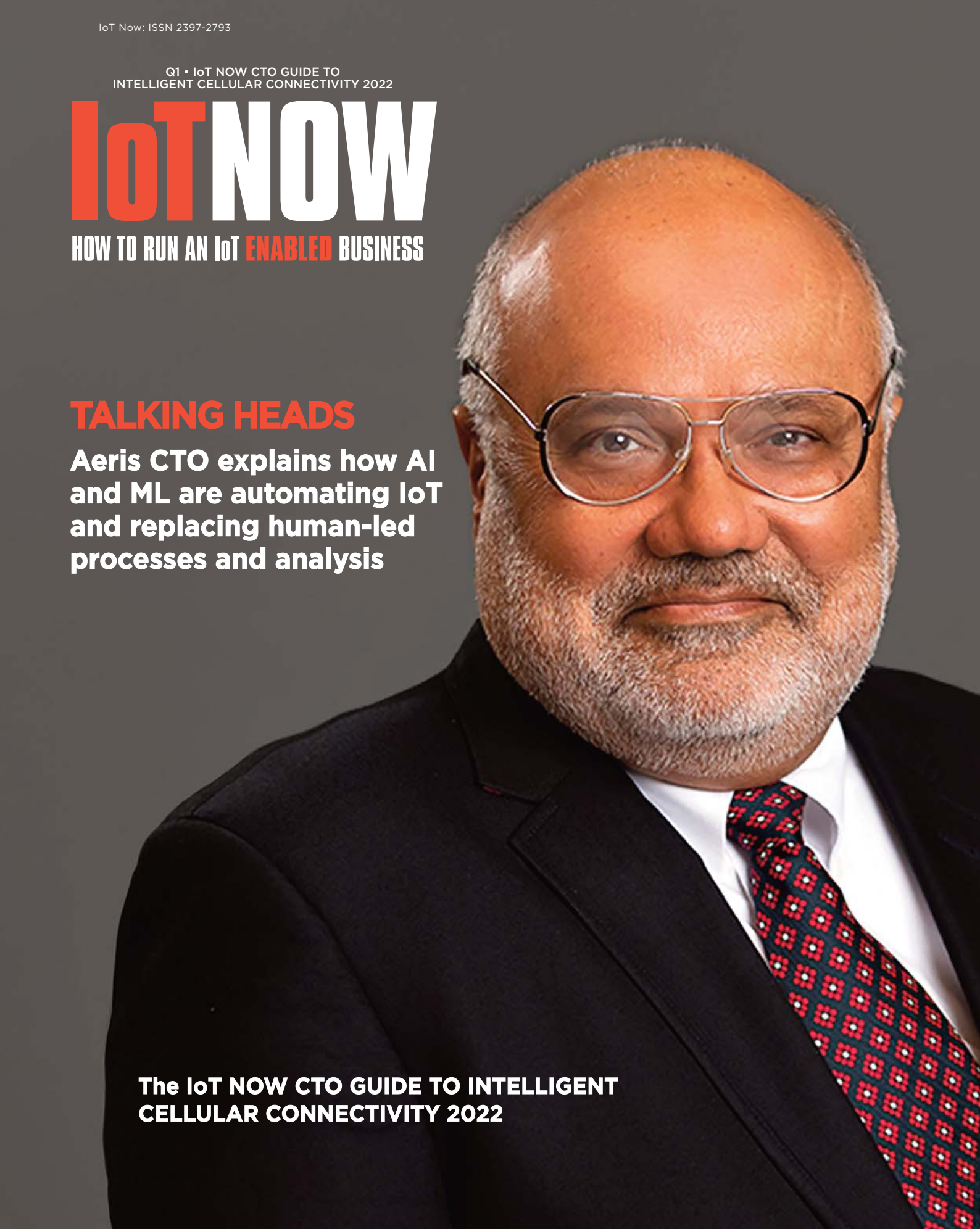
IoT Now: ISSN 2397-2793

Q1 • IoT NOW CTO GUIDE TO
INTELLIGENT CELLULAR CONNECTIVITY 2022

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS



TALKING HEADS

Aeris CTO explains how AI and ML are automating IoT and replacing human-led processes and analysis

The IoT NOW CTO GUIDE TO INTELLIGENT CELLULAR CONNECTIVITY 2022

PLUS: Keep on trucking, keep on tracking with self-installed telematics • Why the cost delta between eSIMs and discrete SIMs must narrow to stimulate mass acceptance • Foresolutions at the forefront of pharmaceutical distribution with multi-carrier coverage • Why eSIM and iSIM can reduce IoT connectivity complexity • Off-grid communities Bboxx clever with connected clean energy services • Why IoT deployments can't afford not to focus on security • News online at **www.iot-now.com**

Have You Seen Our New ‘Succeed With IoT’ Report Series?

Our ‘Succeed with IoT’ report already ranks top of all good internet search engines. Find the series on our new website, along with many other valuable resources.

www.beechamresearch.com

beecham research

Shaping the IoT future

The IoT NOW CTO GUIDE TO INTELLIGENT CELLULAR CONNECTIVITY 2022

IN THIS ISSUE

MANAGING EDITOR
George Malim
Tel: +44 (0) 1225 319566
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 Consultancy Ltd
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

DISTRIBUTION
UK Postings Ltd
Tel: +44 (0) 8456 444137

Printed in the UK by
The Magazine Printing Company
using only paper from FSC/PEFC suppliers
www.magprint.co.uk

IoT Now magazine covers worldwide developments in the Internet of Things (IoT), machine-to-machine (M2M) communications, connected consumer devices, smart buildings and services. To receive ALL 4 ISSUES per year of the printed magazine you need to subscribe. The price includes delivery to your chosen address worldwide. **BUY A 1-YEAR, 2-YEAR, or 3-YEAR SUBSCRIPTION**: **1 Year Normal price UK£60.00 NOW UK£51.00 for 4 issues** OR **2 Years NOW £102 (8 issues, save £18.00) SUBSCRIBE ONLINE**: **www.iot-now.com**

Intelligent connectivity enables carriers to dump the dumb pipe tag

IoT connectivity hasn't been clever. In fact, the constraints of force-fitting national wireless networks designed to serve consumer voice to a rapidly evolving, innovative landscape of connected machines, has been needlessly complex, often dumb and seldom fit for purpose

Now intelligence is arriving and carriers and their partners are harnessing new technologies and finding ways to simplify and add value to IoT connectivity that have the potential to turn it from a bottleneck to an enabler that can supercharge IoT business cases. Increased understanding among carriers that it's better to act as an enabler of IoT than an owner of a customer's ability to connect is spreading and more carriers recognise now that playing a part in the entirety of IoT can be better business than attempting to own a confined area.

Of course, the world's largest carriers still have dominant positions and serve national and even global deployments well. However, IoT is dynamic, composed of moving devices that demand different network capabilities at different times. One carrier is not always the best available in terms of coverage, capacity or cost and therefore the flexibility that embedded SIM and integrated SIM (eSIM and iSIM) are poised to provide will be transformative. Deployments will be able to automatically select the optimum carrier for their needs at any given time.

This utopia of continuous switching between carriers is not realistic today but the direction of travel towards it is established. There are huge advantages associated with this from an IoT device deployment perspective. The SIM is embedded or integrated at the point of device manufacture and no localised configuration is required, thereby radically reducing costs. The eSIM's intelligence enables it to bootstrap its own local connection to a preferred provider and, if it is moved, the process can be repeated.

This enables deploying organisations to ensure they have the connectivity they need to drive forward their deployments. In addition, by moving away from plastic SIMs, security is enhanced thanks to the inherent secure capabilities of eSIM and iSIM. We're truly entering an era of connectivity simplicity and security.

These are foundational capabilities and must be aligned with artificial intelligence (AI) in order that deployments can scale up massively. Manual, human-performed processes simply won't scale up and the data collected by IoT devices needs to be analysed and acted upon rapidly. An intelligent network will be able to automatically handle the complexity and the volumes and is now critical to delivering on customers' expectations, reducing cost and complication and providing the better experiences that IoT promises.

It feels like suddenly intelligent connectivity has made a significant leap forward in terms of simplicity, security and scalability.

Enjoy the magazine!

George Malim

Hardware security modules in demand for secure IoT deployments, says ABI Research

The monolithic hardware security modules (HSM) market has long been locked in its traditional enterprise and payment markets, but the unrelenting expansion of the Internet of Things (IoT) ecosystem has given it wings. **ABI Research** has been tracking the changing market demands that have driven HSM vendors to offer novel delivery models, new integrated form factors, and fit-for-purpose applications, in particular key management and root of trust for the IoT.

The last few years have seen a strong push for the use of HSMs in new vertical markets, especially, those within the IoT ecosystem, including automotive, healthcare, manufacturing and utilities. "By and large, there are three primary drivers for the use of HSMs in these new markets: a growing body of standards and regulatory compliance for the protection of IoT data and devices, functional and physical safety requirements for critical devices such as cyber-physical systems, and finally intellectual property protection," said Michela Menting, the digital security research director at ABI Research.

HSM usage in IoT-centric environments is on the rise particularly in industrial markets

Michela Menting, ABI Research

such as manufacturing and utilities. At the edge, smaller HSMs have emerged that are integrated directly into connected devices, such as trusted platform modules (TPMs) or automotive-level HSMs. Finally, there is also increased demand for HSMs on the backend to process, manage, and secure data coming from those edge devices.

"The HSM offerings targeted at IoT applications focus on offering flexibility without exponentially increasing costs or requiring additional hardware," added Menting. "The diversity in deployment and delivery models is driving penetration and expansion into new target markets, and continued evolution and adaptation of HSM product lines by vendors to these new incoming demands is driving great innovation in the HSM market."

US businesses show IoT investment resilience despite pandemic

According to end user research carried out by **Strategy Analytics** on the US IoT Market in Q2 and Q3 2021, IoT spend as a portion of IT expenditure was higher on average among US companies in 2020 than previously. The research uncovered that 16% of IT decision makers in the US will spend over US$1m on IoT projects over the next year, rising to just under a quarter of respondents in a 1–2 year timeframe.

According to Andrew Brown, the executive director of enterprise and IoT research at Strategy Analytics and author of the report: "The US has weathered the pandemic storm as effectively as any major market, with higher average spending on IoT than a number of other major markets. Of course, business needs swung back towards short term planning and operational spending, with delays on strategic IoT planning as a direct result of the pandemic, but we see serious investment in 5G, which will have a massive impact on IoT environments in the US in the next 12 months and will be by far the most prominent technology added."

David Kerr, the senior vice president of global wireless practice at Strategy Analytics, added: "Security remains the primary barrier to deploying IoT, while unpredictable costs and the challenge of managing IoT networks and devices as deployments begin to scale are concerns among US companies. Having the right skill sets that are needed to deploy IoT effectively is vital. US companies struggle with having the right in-house resources and have an acute need for partners who have the knowledge and experience to make a deployment effective and successful."

European smart gas meter penetration hits 33%

The installed base of smart gas meters in Europe amounted to 39 million units in 2020, equal to a penetration rate of 33%, reports **Berg Insight**. The installed base will continue to grow at a compound annual growth rate of 10.1% between 2020 and 2026, reaching 70.1 million units at the end of the period, the firm predicts.

Annual shipment volumes amounted to 6.5 million in 2020 and are expected to stay at similar levels during 2021–2022 before gradually decreasing along with the completion of several large-scale nationwide roll-outs. Italy, France, the UK and the Netherlands were the most active markets in 2020, together accounting for more than 95% of all smart gas meter shipments during the year.

IoT set to overtake cloud as primary Industry 4.0 technology

New research by **Inmarsat** has revealed that investment in the Internet of Things (IoT) is set to overtake cloud computing, next generation security, big data analytics and other digital transformation technologies in the near future. Respondents drawn from multiple industries reported plans to invest the greatest proportion of their IT budget on IoT projects over the next three years.

IoT has reached a high level of maturity across most organisations, with businesses across all industry sectors now planning to spend an average of US$2.8m on their IoT investments through to 2024. While IoT accounted for an average of 7% of an organisation's IT budget between 2017 and 2020, businesses are planning to spend 10% of their IT budgets on IoT projects over the next three years.

AI must play the role of a human being but in an automated way

As the Internet of Things (IoT) scales up, manual processes and analysis performed by human beings become unviable because of the increasing amount of data. This has resulted in growing demand for greater automation and speed of response in order to head-off issues early enough to avert disaster. These issues range from security to software or firmware updates that contain previously undiscovered bugs. The concept of network intelligence paired with advanced data analytics is a means by which IoT organisations can address their need for speed as Syed 'Z' Hosain, the chief technology officer and co-founder of Aeris, tells Robin Duke-Woolley, the chief executive of Beecham Research

Syed 'Z' Hosain
Aeris

RD-W: We're going to talk about the use of artificial intelligence (AI) for network operations. Before we start, there is a lot of confusion in the market about the differences between AI, machine learning (ML) and deep learning (DL). Can you elaborate on that?

ZH: The differences are subtle. AI is the most general term, combining large amounts of data with fast, iterative processing and intelligent algorithms to learn from patterns or features in data and then apply actions as part of an automation system. ML is a subset of AI focusing on a specific learning task. DL is then a sub-set of ML, for example by using neural networks to rapidly determine which data is most relevant to analyse instead of being instructed. ▶

SPONSORED INTERVIEW

The ultimate goal of AI is basically to take the actions necessary because human beings simply will not have the time to respond quickly enough in a practical way

RD-W: What is network intelligence and how does that relate to AI and ML?

ZH: With network intelligence, we're trying to achieve certain key objectives. First, how can we optimise resource utilisation associated with the network? It's not just about systems, it's also about the people involved. We want to make sure that manual approaches are not a key method that people use for managing their data.

The reason is that the number of devices and the number of data sources generating the input for all of these AI and ML systems will just keep increasing dramatically, to the tune of billions of IoT devices. There is no way human and manual approaches will scale to make that work and achieve the success needed. So what are we trying to do? We want to understand what's happening. We want to learn about what's happening, and then we want to provide that information after we analyse it and make recommendations for action.

The ultimate goal of AI is basically to take the actions necessary because human beings simply will not have the time to respond quickly enough in a practical way. Clearly, network intelligence requires use of standard data analytics techniques, including machine learning for understanding what's important, finding the patterns, and then using the AI methods to implement automated actions.

RD-W: Why do you think this is needed?

ZH: Within the next few years, we're going to start seeing billions of IoT devices deployed, generating a ton of data. Right now it's very easy for a company to deploy ten or a hundred, or even a thousand devices, and monitor them with human techniques to watch the data and see what's going on, selecting whatever metric you prefer. Remember that if you need to go out and touch a device to fix a problem, it's incredibly expensive. You can imagine what could happen if you have millions and even billions of IoT devices deployed out there. Scaling to meet the challenge is needed with more autonomous methods.

RD-W: Do you envisage key steps in achieving that?

ZH: We've defined network intelligence as having six key levels, six stages, if you will, which are: observability, reporting, description, prediction, prescription and then autonomy.

I'll explain what I mean by these terms. First, you start with observability. You make sure you have data available that you can observe and then you report on that. You then need to be able to describe that data in context. Next, you predict what might happen based on what you're seeing. You then prescribe solutions, which a human being could respond to. Ultimately, you achieve the autonomy of an AI solution where that prescription is implemented automatically.

I emphasise it's very important not to skip any of these stages. It is tempting to do that – you see some data, you create a simple rule from that data and you immediately follow through with an action. The human being can then act on behalf of the application data that's coming in. But that's the problem. You really need to understand the amount of data that's coming in, analyse it properly, recognise there may be some patterns that you, as a human being, may not see which a machine can interpret for you. In the appropriate business and application context, those steps become even more important.

RD-W: How significant do you see this as being for areas like IoT security?

ZH: Absolutely essential. We constantly ignore the issue of scale. When you have one device, it's simple. When you have 10,000 or 100,000 or even a few million devices that could get breached in the same identical way, you have a situation where the issue of scale is paramount. You need to be able to watch out for the subtleties of the security issues that might have occurred. That is too difficult for a human being to keep up with.

You have to analyse and learn from the data. You've got to achieve the recognition that a ▶

We have known a situation where a firmware update had a bug in it that essentially caused all devices to get online when they shouldn't have and racked up significant network charges

You probably don't need AI for relatively small systems, but you certainly need it when systems get larger

problem exists and then you have to take action. That action may need to be automated in ways that a human being doesn't necessarily have the means to deal with.

It's a question of the number of devices involved, the complexity of what needs to be done, and the speed it all needs to be done at, to avoid a wider problem and potentially very high cost. AI makes a lot of sense in that scenario. It plays the role of a human being but in an automated way, much more quickly and at scale.

RD-W: Is the ability to deal with a situation quickly and at scale at the heart of this?

ZH: Exactly! You probably don't need AI for relatively small systems, but you certainly need it when the systems get larger. It's all related to the continuing fast growth of IoT and how you manage the infrastructure in a secure way cost-effectively moving forward and at speed.

RD-W: Can you give an example of the need for speed?

ZH: I'm going to use an interesting illustration of the issues involved from a few years ago in the cellular world, where you would see people obtain the information associated with a set of cellular devices. Once they did that, they would immediately distribute that information onto websites where people were just waiting to be able to use it to clone cellular services, and then use them for the general purpose of essentially making free calls.

Someone I spoke to at the cellular company, who was responsible for security, pointed out that the first half an hour or so was absolutely critical. This is because after that time, a given breached, single, cloned number could result in millions of dollars of damages if they didn't take action soon enough. The speed of response was hugely important. Making sure you understand how these network intelligence systems can help you make those predictions and take action is absolutely essential.

RD-W: Where else in the network environment beyond security do you see this use of intelligence as increasingly important?

ZH: AI has a major part to play in connectivity management and in device management as well. You need to quickly identify where and when things may be going wrong and, if they are, to deal with them quickly and at scale. An example of this is updating firmware to a large population of devices.

We have seen a situation where a firmware update had a bug in it that essentially caused all devices to go online when they shouldn't have and racked up significant network charges. It ended up creating a massive data bill for the user – in millions of dollars.

That was bad enough, but as device populations grow, the opportunities for those types of situations to arise in unexpected ways also increases. Again, it's a scaling issue and concerns how to manage unexpected situations that could multiply quickly. This is even more important as IoT becomes more mission critical to enterprise operations. For example, it may not be the correct answer to just disconnect devices automatically if they start to use more data than expected. The situations will become more complex and need to be analysed and handled quickly and effectively at scale.

RD-W: What is Aeris doing about this?

ZH: At Aeris, we're working on this now. Our network connects millions of IoT devices across the world. We carry an average 1.5 billion IoT ▶

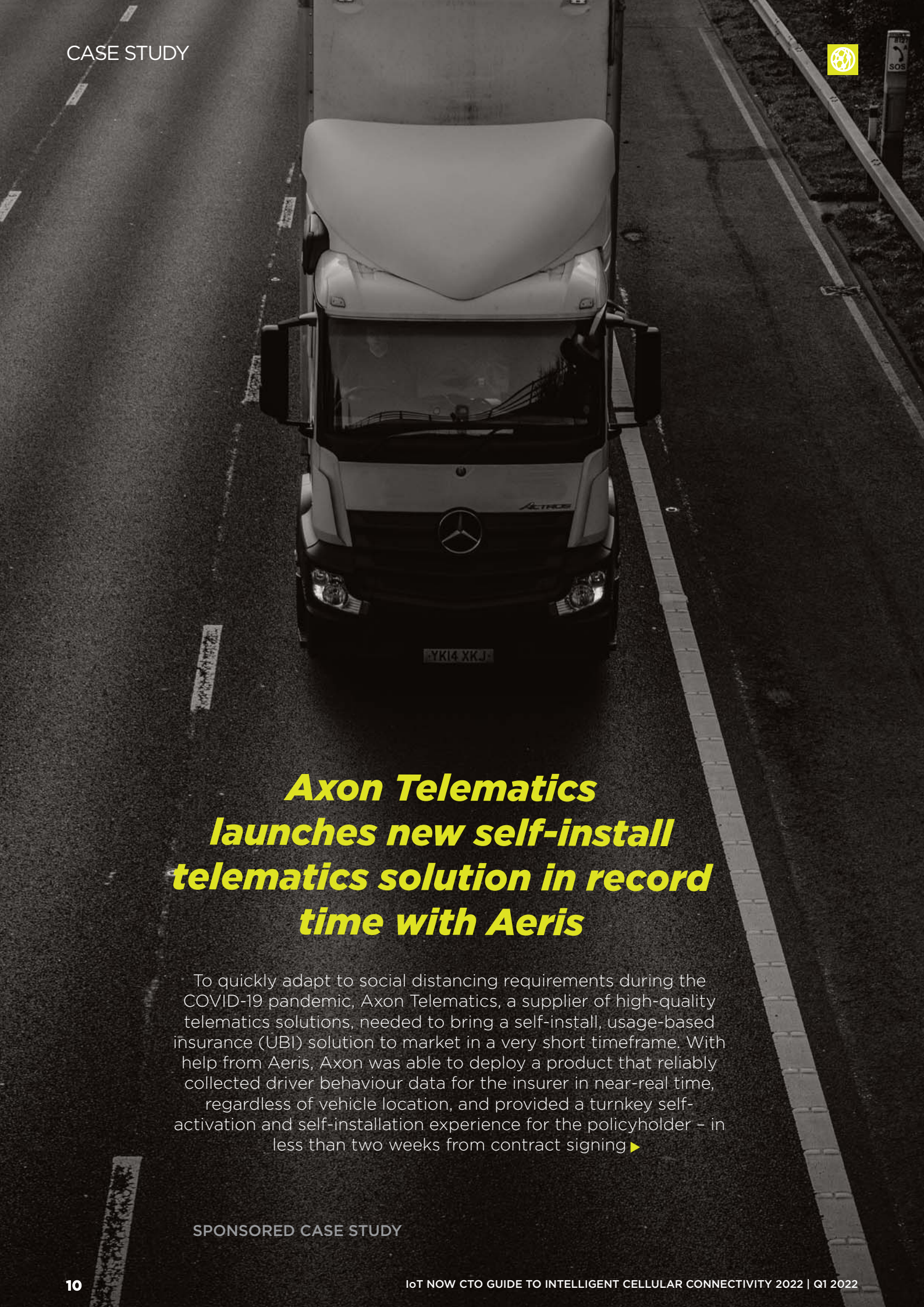
The bottom line is that without an intelligent IoT network, you're going to have difficulty delivering better experiences

messages per day. We have been conducting detailed data analytics on this traffic for some time and now introducing AI and network intelligence to take us forward. The key thing is this: IoT won't achieve its goal of growth if it cannot scale. AI is an enabler of growth for IoT. 5G is also a huge enabler for IoT growth. The two go together.

In summary, what an intelligent IoT network does is it works on your behalf. You're going to get the better security, the better performance and reliability you want from your programmes and applications. These deployments continue to grow in complexity. If you have only a manual system, you're going to add to your IoT application deployment's inefficiency and cost. I always recommend, don't go it alone, get the data scientists on staff, or find a good partner like us to help you make those right decisions.

The bottom line is that without an intelligent IoT network, you're going to have difficulty delivering better experiences, reducing your complexities, and really getting the desired business results for your IoT applications.

www.aeris.com/intelligentIoT



Axon Telematics launches new self-install telematics solution in record time with Aeris

To quickly adapt to social distancing requirements during the COVID-19 pandemic, Axon Telematics, a supplier of high-quality telematics solutions, needed to bring a self-install, usage-based insurance (UBI) solution to market in a very short timeframe. With help from Aeris, Axon was able to deploy a product that reliably collected driver behaviour data for the insurer in near-real time, regardless of vehicle location, and provided a turnkey self-activation and self-installation experience for the policyholder – in less than two weeks from contract signing ▶

SPONSORED CASE STUDY

Axon Telematics focuses on supplying high-quality data enrichment, data quality metrics, flexible reporting and driver scoring to the insurance industry. Headquartered in London, Axon uses its extensive experience and cutting edge data processing platform to build bespoke solutions for insurers and other automotive related businesses to provide real-time insights.

Requirements for rapid launch

To deliver a completely turnkey service that would eliminate the need for a technician, Axon required automated SIM provisioning and activation from a single interface. A self-installation process must be simple and frustration-free, so Axon needed to ensure broad coverage that would facilitate the installation wherever end users are located. To get to market quickly, Axon needed a commercial model that reduced financial risk to secure internal approval, as well as expert service to assist with solution configuration and testing.

Deploying with Aeris

Having already partnered with Aeris on a prior project, Axon knew Aeris offered the blend of technology and expertise to help it respond quickly to an unexpected opportunity. Through collaboration between the two companies, Axon was able to achieve the following key benefits:

Rapid launch: Aeris' application programme interfaces (APIs), which enable automatic provisioning, activation, deactivation and suspension of SIMs throughout their lifecycle, enabled Axon to rapidly deploy a turnkey product that end users could install on their own without needing to interact with a technician. Aeris' white-glove onboarding support included device configuration and testing assistance, enabling Axon to launch in a matter of weeks.

Superior coverage: Aeris' performance-optimised, multi-carrier coverage eliminates reliance on a single network provider, ensuring near real-time transmission of data regardless of device location. Axon can be confident that policyholders will be able to register easily and activate their devices wherever they are.

Attractive cost structure: Aeris' pay-as-you-go plan removed the financial risk of overages for Axon so it wouldn't have to pay for data its customers don't use. A flexible payment plan made it faster for Axon to gain internal approval and quickly launch the solution.

"With Aeris, all of our services are managed in-house, ensuring we can maintain quality from provisioning, installation, operational management, and end of life process – something we really struggled to do with our previous supplier," says Matthew Wilcox, the chief technology officer at Axon Telematics.

Into the future

Axon knew it was crucial to select a connectivity provider who would not just help it launch quickly, but would continue to be a partner after deployment. Based on its previous experience with Aeris, Axon felt confident in expanding its partnership. The Aeris Intelligent IoT Network provides performance-optimised coverage from 600 carriers in 190 countries and end-to-end visibility and control over Axon's entire connected operation, enabling Axon to deliver superior quality of service to its customers while optimising costs across their businesses.

On an ongoing basis, the Aeris Intelligent IoT Network will provide Axon with:

Improved quality of service: Aeris' automated monitoring of device connection status and remote diagnostic tools will enable Axon to proactively detect and address any potential issues, ensuring the highest possible quality of service for both the insurer and its policyholders.

Increased profitability: The pay-as-you-go rate plan that helped Axon secure quick approval for the project will also continue to pay dividends for years to come. Axon only pays for data that is used, reducing its underlying costs and enabling it to offer more attractive cost structures to its insurance customers.

Future growth potential: The broad coverage offered by the Aeris Intelligent IoT Network ensures that not only can Axon's new solution be confidently deployed today, but it can be expanded in the future as new opportunities present themselves in other geographies.

www.aeris.com/IntelligentIoT

eSIM understanding grows as cost delta narrows

Embedded SIM (eSIM) promises huge simplicity alongside improved security and greater management control. However, these benefits come at a cost and eSIM isn't for everyone – yet. Drew Johnson, the executive vice president of product and technology at Aeris, tells IoT Now managing editor George Malim, that eSIM has real advantages for manufacturers that distribute globally but the cost delta between eSIM and discrete SIMs needs to narrow further before ubiquitous adoption becomes a reality

George Malim: As organisations look to simplify provision of global IoT connectivity for their deployments, what approaches are they taking to limit the number of vendors they interact with and to make the process of onboarding easier?

Drew Johnson: This question hits upon the underlying tension of the eSIM trade-off which is between the need to deliver simplicity and the complexity of involving multiple carriers. If you're going to integrate with two or three underlying carriers, you can blow away simplicity very quickly.

We look at eSIM as a technology enabler, it's not really a solution. Customers already have a level of freedom to operate everywhere, and we have customers that use us to operate their solution anywhere in the world. What they get along with our eSIM is this intelligent platform to work with carriers globally. Through our intelligent IoT connectivity platform, they get actionable intelligence that enables them to have more secure connectivity, better coverage, and greater cost controls, plus the added benefit of superior support intelligence from our customer support organisation. It's really about our intelligent platform as an enabler that helps deliver on the promises of the eSIM technology.

What many in the industry have failed to sufficiently acknowledge are the business issues with unmanaged eSIM. More specifically, the multiple carrier relationships and integrations you are going to have to address during the onboarding process. A key selling point is adding a new carrier profile via over-the-air (OTA) update. However there is an integration effort involved each time a new carrier profile is added. On top of this complexity, organisations need to attain a level of security and diagnostics capabilities, and transparency is needed for end-to-end monitoring. With **Aeris**, you get one onboarding with one consistent platform and one set of security, cost control and onboarding mechanisms. That is the difference we bring.

GM: eSIM has been seen for many years now as a means to enable devices with global connectivity. How are you seeing eSIM acceptance accelerating?

DJ: We've been looking at or working on eSIM since 2014. There have been various impediments to mass adoption. That explains why it has taken so long for eSIM to gain market traction. We have witnessed this first-hand in our support of eSIM with connected cars, where adoption was slow at first. Now the adoption is accelerating and the reality of eSIM is starting to catch up with the hype. However, there have certainly been incidences that show how misinformation has hampered uptake.

Having said that, there is now a set of use cases, particularly for manufacturers of distributed connected things that don't know at the point of manufacture where their IoT devices will be deployed. These are a perfect use case for eSIMs and I think it's fair to say that customers have become more educated about eSIM generally. In fact, we learned from our most recent eSIM webinar that a good portion of our audience already have exposure to eSIM. However, some still think eSIM is the solution to all their dreams, but this isn't necessarily the case.

GM: What further is needed for increased adoption of eSIM in IoT?

DJ: We see three main enablers of greater eSIM adoption. The first is the carrier business relationship. This has accounted for a fair amount of the impediment to greater eSIM adoption. However, as the market has matured, larger volume deployments have arrived that make it practical and attractive for carriers to support. For example, big automotive manufacturers now have large enough deployments to get eSIM off to a fast start. Through these engagements with automotive manufacturers, Aeris has mastered the business rules to support delivery of eSIM and the necessary underlying carrier agreements.

The second aspect is the cost delta between eSIM and traditional plastic SIMs. In IoT, cost is really important, especially if you can get the cost of eSIM down to a level where it is viable for smaller volume IoT use cases. The cost delta relative to discrete SIMs has become smaller with eSIMs. The smaller the cost delta, the larger the uptake of eSIMs obviously will be.

The third point is simplicity, which is critically important for organisations that want to ensure that security, support, coverage, costs and control are maintained consistently across all the underlying carrier relationships. If the platform is too complex, everything can fall apart very quickly.

GM: What is Aeris' approach to eSIM with your the Aeris Intelligent IoT Network?

DJ: We have a portfolio of robust carrier relationships available today. We ▶

With Aeris, you get one onboarding with one consistent platform and one set of security, cost control and onboarding mechanisms. That is the difference we bring

Drew Johnson
Aeris

have carefully chosen multiple reliable relationships and packaged them in a way that is optimised for manufacturers that have a global customer footprint. That's where we applied network intelligence to make our eSIM solution unique. It also enables our customers to extract the most and the best value from the eSIM technology right now.

The Aeris Intelligent IoT Network gives customers the freedom to operate anywhere in the world. It's now the case that manufacturers want to make and distribute anywhere in the world with a connected product that just works wherever it is deployed. We are delighted to be able to help our customers meet that need and have the freedom to operate globally.

If in a rare instance our eSIM solution doesn't provide the connectivity our customers need in a particular spot in the world, or if they simply want to change to a different carrier, we can help our customers add new ones or move to another carrier. It's this type of flexibility that really adds value and simplicity.

GM: How do your customers benefit from eSIM capabilities within the Aeris Intelligent IoT Network?

DJ: What customers are looking for is a single onboarding mechanism and a single platform that are able to continue to deliver security, support, and coverage capabilities. Intelligence around the coverage is also important so that no matter where the IoT device wakes up anywhere in the world, it can connect to the cellular network that is most suitable for the specific use case. Customers want that assurance and we are able to offer them the confidence as they scale up their IoT deployments around the world.

GM: Do you see eSIM as the enabler of radically simplified global IoT connectivity?

DJ: Enabler is the important word. eSIM is an enabler technology because it's necessary but not sufficient in itself. What's equally important, perhaps even more crucial, is an intelligent platform that will actually deliver the radically simplified global IoT connectivity that organisations have been waiting for since the concept of eSIM was first introduced.

We have had customers saying they really want eSIM, but once they learn about all the important details such as onboarding, management, security and others, eSIM turned out to be not the best option for them. They often ended up with a set of discrete SIMs because their supply chain is organised in such a way that the end destination may be the best place to install SIM capability. Or maybe it's because the IoT-enabled device does not need to be used across different geographical regions. In those situations, the added cost of eSIM does not offset the extra benefits eSIM can deliver.

I believe that the cost delta between eSIM and discrete SIMs will approach zero in the future. When that happens, there will be an inflection point where eSIM becomes a ubiquitous offering, but we are still some time away from this. ■

www.aeris.com/IntelligentIoT

Foresolutions reduces operational costs with performance-optimised multi-carrier coverage and remote issue diagnosis

Foresolutions, a provider of tracking solutions to a variety of different sectors, has used the Aeris Intelligent IoT Network to serve the needs of customers in the pharmaceutical sector. The Aeris Intelligent IoT Network makes it possible for Foresolutions to consistently track the location and temperature of vital medical supplies in real-time, as they are transported throughout Europe

Located on the south coast of England and servicing a national network of customers in a variety of sectors, Foresolutions helps business operations professionals who want better results from investment in the communications and tracking technology they use to improve business performance. Foresolutions provides a complete communications solution focusing on cost-effective and performance-generating solutions from mobile phones, IoT and GPS tracking, and two-way radio communications.

To accurately track to assets in transport, Foresolutions requires consistent, reliable connectivity across multiple geographies. To detect anomalies and prevent costly overages, Foresolutions requires complete visibility into the connection status and history of each device. Historically, Foresolutions had endured regular network outages – often triggered by network maintenance – which interrupted visibility into asset location and temperature, creating uncertainty with regards to the health of assets in transport.

"Foresolutions' customers who operate in the pharmaceutical sector transport vital medical products throughout Europe, and it is critical that all of these assets are tracked with zero downtime," explains Nathan Williams, the technical sales director at Foresolutions. "With Aeris, we have found a partner who delivers that network reliability, regardless of geography."

Poor network connectivity and the challenge of tracking assets across different geographies were the central challenges Foresolutions faced. For businesses transporting priority assets across numerous borders, having a reliable connectivity partner is essential to ensure the security and safety of those assets. Foresolutions' customers operating in the pharmaceutical sector are no exception. ▶

SPONSORED CASE STUDY

With an extensive customer base depending on reliable connectivity to ensure critical medications are tracked and monitored in real-time, network downtime and inconsistent connectivity presented significant challenges for Foresolutions. The company needed a connectivity provider who could ensure consistent, reliable coverage across multiple geographies at fully optimised costs.

Beyond a superior coverage footprint, Foresolutions' also required automated tools that would allow it to easily provision, activate, and deactivate SIMs throughout its entire lifecycle; automatically detect device connectivity issues or unusual data consumption; and block service to devices behaving abnormally. In addition to unreliable coverage, Foresolutions' previous connectivity provider offered only limited visibility into device behaviour, allowing data overages to go undetected and racking up of unnecessary connectivity costs.

Why Foresolutions chose Aeris

The primary reason for selecting Aeris was that it offered network reliability for precise tracking and monitoring of all connected devices. With the Aeris Intelligent IoT Network, connectivity is never an issue. Switching networks if the signal strength drops below a defined threshold when travelling outside the geographical coverage area of the home network is among the Aeris Intelligent IoT Network's key attributes. This ensures that there is no downtime or loss of signal so that Foresolutions' customers always have visibility into the location and temperature of pharmaceutical assets.

Network reliability was a prerequisite for Williams: "With Aeris, we have found a partner who delivers network reliability, regardless of geography," he adds. "We can also hold SIMs without charge, as we receive notifications in the event of over usage and can switch billing on and off as required."

The results

Maximum performance: The Aeris Intelligent IoT Network eliminated reliance on a single network provider, ensuring uninterrupted visibility as tracked assets move across different territories.

Lower operational costs: The Aeris Intelligent IoT Network's automated solution monitoring and near real-time alerts significantly reduced the amount of time and resources needed to manage and monitor device connectivity.

Cost-effective SIM management: The Aeris Intelligent IoT Network provides end-to-end visibility into and control over SIMs throughout their entire lifecycle, allowing Foresolutions to easily control costs, streamline operations and provide turnkey service by automatically activating and deactivating SIMs as devices come in and out of operation.

Since Aeris develops, owns, and operates its own core network, which controls all device and network interactions, Aeris is able to provide end-to-end visibility into and control over the behaviour of all devices on the network. The Aeris Intelligent IoT Network provides a single-pane-of-glass view into the connection status and history of all of Foresolutions' devices – regardless of the carriers or technologies to which they are connected – and provides automated solution monitoring with real-time alerts to help Foresolutions rapidly detect, diagnose, and respond to issues anywhere in its end-to-end system. Finally, the Aeris Intelligent IoT Network also makes it possible for Foresolutions to easily, automatically activate and deactivate SIMs as they come in and out of operation, simplifying connectivity management and reducing costs.

"With the Aeris Intelligent IoT Network, we have visibility into all of our SIMs and their data usage and can make adjustments at a moment's notice," concludes Williams. "In addition, we can monitor multiple devices' consumption levels and traffic patterns, and diagnose and resolve anomalies or issues, all in one clear, concise tool. The support that we have received from Aeris has been exemplary." ■ **www.aeris.com/IntelligentIoT**

How eSIM and iSIM are reducing IoT connectivity complexity

Embedded SIM (eSIM) has emerged as a means to free consumers and connected devices from the constraints of the traditional, plastic subscriber identification module (SIM) card by enabling an eSIM or an integrated SIM (iSIM) to be embedded into a device at the point of manufacture and shipped globally. On arrival at the location where it will be used, the device simply connects to the most suitable network operator in a process known as bootstrapping and the device is authorised to connect to the network, with the owner paying service charges. That's the theory at least, reality will involve some fragmentation and the need to select providers and manufacturers that can integrate or embed SIMs into devices, writes George Malim

The promise of this radically simplified process is an advantage for original equipment manufacturers (OEMs) because it enables them to streamline the production process and have just a single stock-keeping unit (SKU) designation for a global product rather than having multiple variants for different global markets. They'll also be able to play themselves into the connectivity value chain, potentially using their customers and the volumes of devices they make as a springboard to negotiate deals with connectivity providers that they can resell to customers.

User organisations will also benefit because they won't have to install SIM cards into devices when they arrive at the point of use. In addition, they won't have to configure simple devices for local markets, saving time and cost. These organisations won't have to engage in complex vendor management processes nor have to commit to a single carrier for the life of the deployment. Instead, they will have flexibility to choose the best coverage at the best price for each deployment – and, in future, to shift operator when this is no longer optimal.

The SIM revolution is already underway as **Figure 1** shows. **Strategy Analytics** forecasts that sales of eSIMs for IoT applications will grow to 326 million by 2025. One of the reasons for this projection, according to the firm is that eSIM offers the ability to change service provider profiles using remote SIM provisioning (RSP), without needing to physically change the SIM card itself, which is vital in enabling devices where it is either difficult or inefficient to access a physical SIM, for example ▶

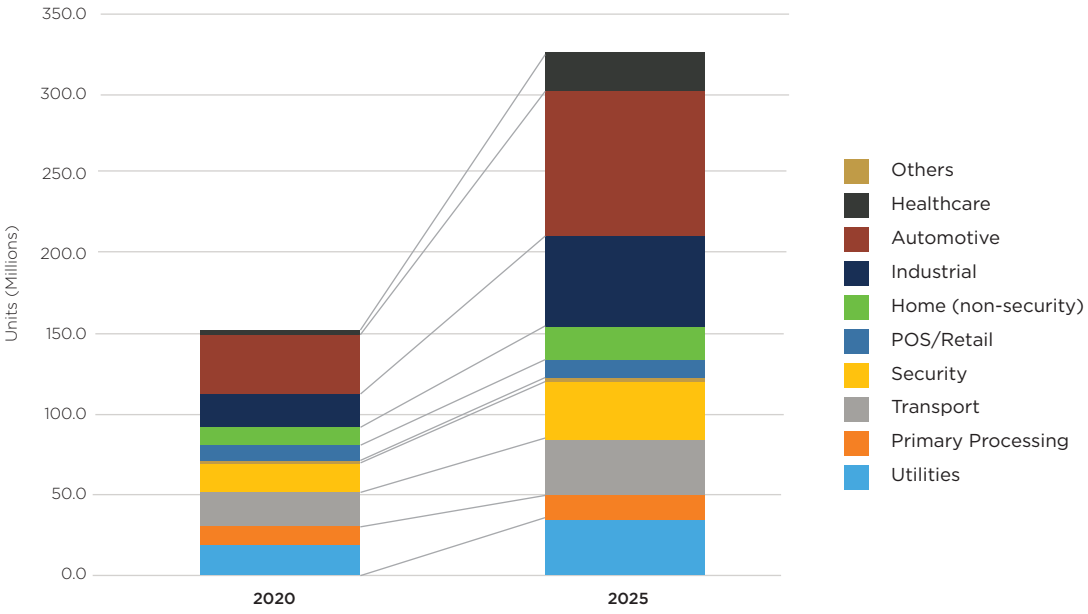


Figure 1: Total IoT eSIM sales by vertical industry (millions)

Source: Strategy Analytics, 2020

hermetically sealed medical devices, vehicles, consumer electronics devices or a whole range of other IoT devices.

RSP also plays into IoT organisations' desire not only to have flexibility but to have greater control of connectivity and to be assured of security for their devices. Significant steps have been made in this respect with **GSMA** piloting development of the IoT SIM Applet For Secure End-2-End Communications (IoT SAFE), which aims to provide a standardised, globally accepted root of trust for IoT communications. Ensuring that eSIM includes a root of trust or secure element is therefore an increasingly important requirement and one which suppliers are responding to.

Traditional credentials, such as smart cards, will continue to account for the majority of market volume although the ability to create, access and share digital credentials, plus securing connected devices, will drive adoption of higher value solutions. Even so, adoption of eSIM in IoT is only expected to account for a small portion of overall eSIM adoption.

Although it does not foresee the industrial and public sectors driving eSIM uptake, **Juniper Research** does see significant opportunities for the technology across industrial sectors. A recent study by the firm identified the oil and gas, manufacturing and logistics sectors as three key areas in which eSIM adoption will ramp up. eSIM installations in these verticals grow from 28 million units in 2021 to 116 million by 2025. The firm's research also suggests that the development of rugged devices and appealing form factors will position vendors well to capitalise on the market.

In spite of this significant growth, Juniper Research believes it is the consumer sector▶

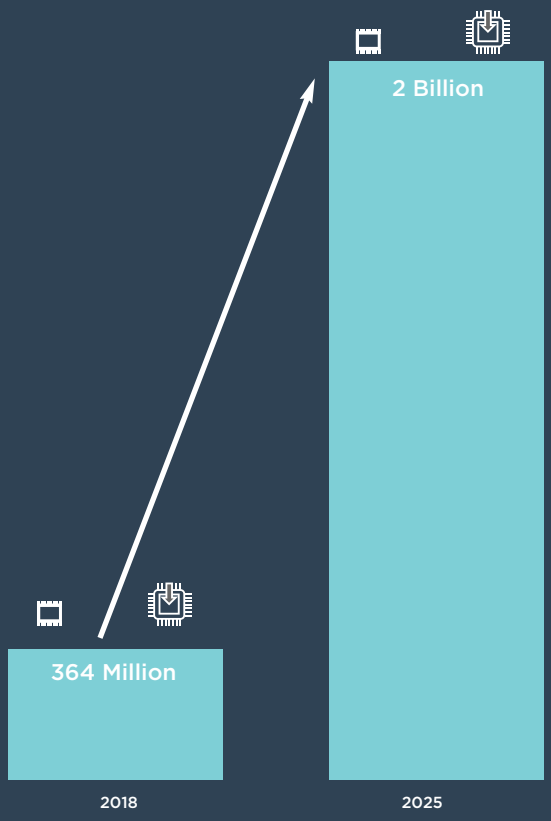


Figure 1: Global eSIM-based* device shipments: 2018 vs. 2025 % growth

Source: Counterpoint Research – Global eSIM Tracker and Forecast – 2018-2025
*includes all eSIM form-factors – hardware, soft/virtual and integrated

that will account for 94% of global eSIM installations by 2025 and it anticipates that established adoption of eSIM frameworks from consumer device vendors, such as **Apple** and **Google**, will accelerate the growth of eSIMs in consumer devices ahead of the industrial and public sectors. The bulk of eSIMs will be installed in connected devices and these will increase from 1.2 billion in 2021, to 3.4 billion in 2025; representing a growth of 180%.

The research also uncovered that global eSIM deployments across all consumer verticals will increase by 170% over the next four years, with widespread adoption reliant on backing from network operators. Juniper Research therefore has urged device manufacturers to place pressure on operators to support eSIM frameworks and accelerate market maturation.

The fragmentation that exists between hardware vendors in the cellular IoT device market will require each vertical to adopt a combination of wireless technologies, hardware and management tools. In time, specialist vendors will emerge that provide robust eSIM form factors for industrial environments. These, alongside eSIM and iSIM providers that adopt secure practices and enable the new SIM to become a root of trust, will empower IoT – as well as other sectors – with secure and flexible means to connect their devices with less friction and more choice than ever before.

With eSIM adoption already underway, it is expected to be adopted within smartphones, enterprise IoT and wearables, with integrated iSIM technology following by 2025. **Counterpoint Research** has estimated shipments of eSIM-based devices will reach almost two billion units by 2025, up from 364 million in 2018, according to the latest research from the company's Emerging Technology Opportunities Service. The findings also show that a majority of eSIM-based devices will have a hardware chip-based eSIM solution until 2025 and, after that, there will be a rise in the adoption of iSIM-based solutions. ▶

Adoption of eSIMs in smartphones – again, the consumer market – is expected to drive the major volume growth while other connected devices such as mobile hotspots, routers, connected PCs, drones and smartwatches will grow at a higher CAGR because of their relatively smaller base of adoption today. However, in terms of shipment volumes, smartphones and B2B IoT devices will lead.

Counterpoint expects we will see a shift in adoption to the GSMA-compliant hardware-based embedded universal integrated circuit card (eUICC) for the next five to six years alongside iSIM or iUICC within system-on-a-chip (SoCs) devices across different device categories, replacing the less secure proprietary soft eSIM solutions. While hardware-based eUICC will be popular across smartphones, automotive, iSIM or iUICC will be popular across IoT applications.

Reduced risk

The arrival of eUICC creates an open standard by which connectivity can interoperate and be orchestrated for localisation. This is important for IoT organisations across several dimensions. At its most basic, it enables moving devices to shift location and even country without having to renegotiate for connectivity so it's ideal for asset tracking across a market such as western Europe. That renegotiation could involve installation of a new physical SIM and makes several use cases unviable.

For less mobile, but still movable items, orchestration for localisation means a vending machine can be sited in a garage in Los Angeles and, if the location isn't successful, it can be moved with no fuss to another location where the best mobile network may be from another provider. The vending company doesn't have to worry about the connectivity, only its business case of making sure its machines go where the most customers are.

This capability also takes away the risk involved in connectivity selection. If you know you can reconfigure device connectivity over-the-air, you know you are in control of your device. This is especially important for devices with long operating life expectancy that might be in the field for many years.

For these types of deployments, having to make network selections today for a device that might still be active in 2030 is a significant worry. No one knows what the connectivity landscape may look like then and being tied to a connectivity contract from 2020 provides no flexibility to respond to changing market needs.

A further concern that intelligent connectivity addresses are the dynamics of the global economy. Different countries impose different regulations and these could render certain approaches to connectivity obsolete. By having one connectivity platform for IoT, organisations can manage these changes by switching operator to ensure an approved form of connectivity is utilised. In addition, they are insulated from geo-political shifts such as if one country has a conflict with another.

By adopting an intelligent approach to connectivity and selecting an IoT connectivity partner that understands the potential eSIM brings but also the need to manage different use cases in different countries in different ways, IoT organisations can ensure they are in a position to continuously have optimised IoT connectivity. Different countries have different regulations – Brazil, for example, does not allow permanent roaming which means IoT devices can only connect using a local carrier.

Therefore, the possibility to keep connectivity streamlined by having a single connectivity platform from one provider is appealing. This platform provider can manage all the changes and handle all the integrations. In addition, deals of this type insulate the customer organisation from changes such as geo-political shifts that might cause an individual organisation to rethink its connectivity provision. eSIM and iSIM are among the most significant innovations to arrive in IoT connectivity in the last ten years, it's now time to engage with them and work out how to make them contribute to your IoT project. ■

With Aeris, Bboxx provides clean energy solutions to off-grid communities and those connected to an unreliable grid

Companies operating in the most remote locations, with products purpose-built for off-grid, rural, and often hostile environments, as well as people who are connected to unreliable grids in peri-urban or urban areas, require a reliable global mobile network. This must provide consistent connectivity worldwide to enable effortless remote monitoring of energy systems. To overcome many life-critical energy-delivery issues there is significant need for reliable GSM and CDMA connectivity to deliver functional energy saving solutions

Currently, 759 million people live without access to energy, of which 570 million are in Africa. An additional 840 million people are connected to an unreliable grid.

The United Nations Foundation has stated that "energy powers the world's economic engine," adding that, "from the perspective of jobs, security, climate change, food production, or increasing incomes, access to sustainable energy for all is essential for strengthening economies, protecting ecosystems, and achieving equity."

Bboxx transforms lives and unlocks potential

Bboxx is a next generation utility providing affordable, reliable and clean electricity and other utility services to millions who are living without power, transforming lives and unlocking the potential of communities, cities and countries. Bboxx designs, manufactures, distributes and finances innovative plug-and-play solar powered systems to improve access to energy across Africa and the developing world. Bboxx exists to solve global energy poverty. ▶

SPONSORED CASE STUDY

Through a vast network of shops and outlets, Bboxx focuses on providing people access to electricity, while offering superior customer service. Its core products are a range of solar-powered systems that sit in a home or at SMEs and allow users to power appliances, such as lights, torches, mobile phone or laptop chargers, refrigerators, TVs, radios, fans or shavers.

Bboxx needed to use real-time data to identify device issues early — with proactive alerts sent to customer service agents to ensure that system problems could be fixed before they evolved. Because of this, the company required a reliable cellular network that enabled effortless remote monitoring and access to real-time data, as well as the ability to configure and adapt each system so as to maximise battery life and provide cost-effective solutions for both itself and its customers.

"By working with Aeris, we can ensure that our solutions have optimum reliability, and our customers can be sure their devices possess a reliable connection, at all times, no matter the location," says Christopher Baker-Brian, the co-founder and managing director of the product division at Bboxx. "Aeris' high quality service and IoT expertise ensures that we can offer the best clean energy solutions to people living without access to energy or people connected to an unreliable grid in developing countries."

In addition, Bboxx products are manufactured without a known destination and, as such, with certain mobile network providers, a local SIM card would have to be inserted into the device following sale and then would require local configuration. This process required additional time, cost more and hindered operational effectiveness. Therefore, mass global deployment of solutions only was possible by working with a reliable cellular network partner that provided end-to-end monitoring, no matter where in the world systems are deployed. Bboxx also needed a partner that could connect to multiple carriers, regardless of location.

The Aeris IoT solution

Aeris offers multiple, non-steered network connectivity in East and Central Africa, the principle areas where Bboxx deploys thereby enabling real-time gathering of actionable data. Aeris' global support of major cellular technology standards, such as GSM, CDMA and LTE, also ensured that Bboxx could deploy its devices in any location during global expansion.

With the Aeris IoT Services platform, Bboxx can install the Aeris global subscriber identity module (SIM) at the point of manufacture, reducing both supply chain costs and deployment time. Also, by utilising Aeris' single global access point name (APN), the solar-powered Bboxx system could be deployed on a simple plug-and-play basis, without the need to reconfigure to local network settings.

By utilising the Aeris connectivity management platform, AerPort, for IoT devices, Bboxx was able to have real-time access to data usage, alert management, and device connectivity management over the SIM life cycle.

Customer benefits

Aeris IoT Services' network connectivity enables Bboxx to remotely monitor its devices. Configuration and deployment times have been reduced significantly. Predictive and proactive maintenance help lower ownership and maintenance costs and plug-and-play devices can be switched off from a central location if troubleshooting issues arise or if payments are not met. All this adds up to the lowest possible total cost of ownership (TCO) for an IoT solution. **www.aeris.com/IntelligentIoT**

Bboxx

About Bboxx

Bboxx is a next generation utility, transforming lives and unlocking potential through access to energy. Bboxx manufactures, distributes and finances decentralised solar powered systems in developing countries. It is scaling through forging strategic partnerships and its innovative technology Bboxx Pulse, a comprehensive management platform using IoT technology. Through affordable, reliable, and clean utility provision, Bboxx is bringing people into the digital economy, creating new markets, and enabling economic development in off-grid communities and those living without a reliable grid connection. The company is positively impacting the lives of more than two million people with its products and services in over 27 markets, directly contributing to 11 of the 17 United Nations Sustainable Development Goals.

So far, Bboxx has deployed more than 500,000 solar home systems. Bboxx has over 1,000 staff across nine offices including in the Democratic Republic of Congo, Kenya, Rwanda, and Togo, with its head office in the UK and its manufacturing operations in China. In 2019, Bboxx was the winner of the Zayed Sustainability Prize in the Energy category – testament to the way the company is making a meaningful difference to people's lives around the world. You can find further information about Bboxx on its website at **www.bboxx.com/#/about**

Why IoT deployments can't afford not to focus on security

More connections mean a larger target area for cybercriminals to attack but advances in connectivity, hardware and software security are equipping IoT organisations to fight back. The challenge is to balance investment in security with what the business case can stand, writes George Malim

As the number of IoT connections accelerates further into the billions, the volume and diversity of attacks is also increasing, placing greater emphasis on security in IoT organisations' minds as they assess not only the financial cost of breaches but also the impact of reputational damage. Research by security specialist, **Kaspersky**, has uncovered that more than 1.5 billion attacks have occurred against IoT devices in the first six months of 2021. The firm's telemetry data, which it draws from its honeypots that collect attack information, has shown that cyberattacks on IoT devices have increased by more than 100% since the previous half-year.

This reveals that further improvements in understanding of potential threats facing IoT deployments are needed and stronger action to mitigate security weaknesses needs to be taken. However, investment in security needs to be proportionate to the risk and there is a concern that investing too much in IoT security could hinder scalability in future or delay time-to-market now. Bluntly, IoT services need to have sufficient margin to ensure they can be provided securely.

The scale and range of this challenge is well-understood and reflected by predictions of increased spending on IoT security from analyst firms. Research firm **IoT Analytics** projects a CAGR of 44% in spending on IoT security in the period 2017-2022. **Technavio** has also been monitoring the IoT security market and predicts it is poised to grow by US$80.94bn during 2020-2024, progressing at a CAGR of almost 37% during the forecast period.

IoT Analytics' latest update reports that spending on enterprise IoT solutions grew 12.1% in 2020 to US$128.9bn, with the COVID-19 pandemic having different impacts on different segments of the IoT market. For example, spending on IoT ▶

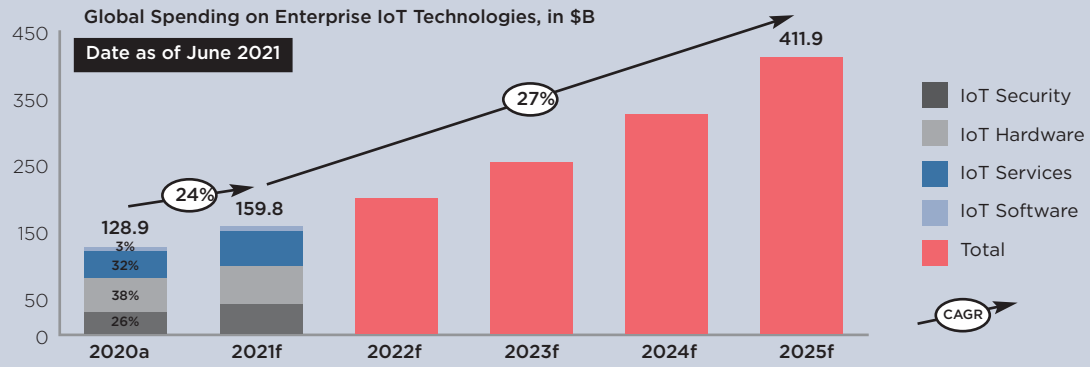


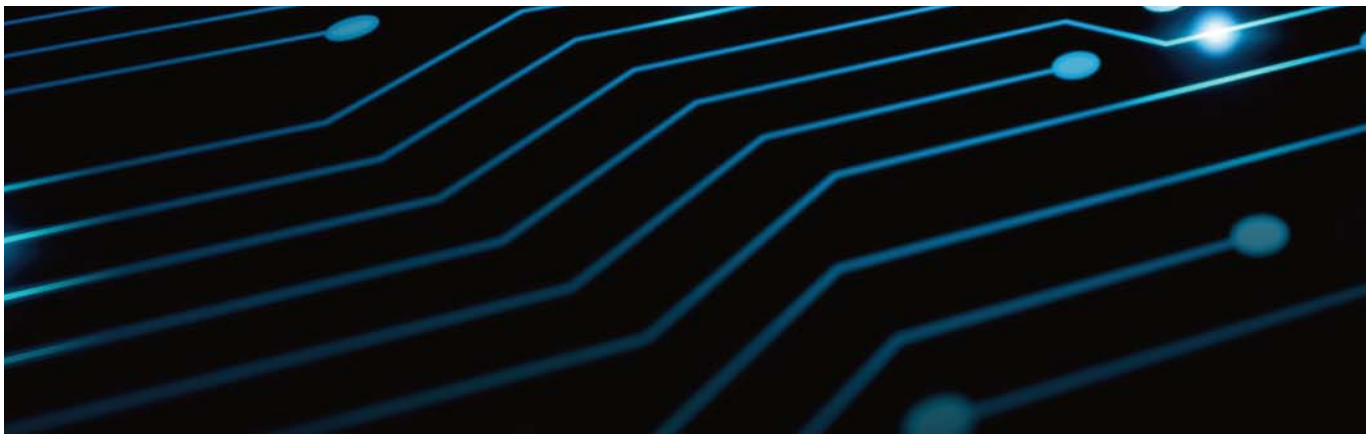
Figure 1: IoT Enterprise spending 2020-2025
Source: IoT Analytics

hardware grew 5.4% in 2020, while spending on IoT cloud and infrastructure services grew 34.7% in the same timeframe. Many hardware installations were postponed as travel came to a standstill and capital expenditure budgets were frozen.

Nevertheless, companies increased their spending on IoT security in 2020 by 40.3%. This sounds massive but is still just 3% of total enterprise spending on IoT solutions, as shown in **Figure 1**. The surge in high-profile security attacks led companies to increase spending in the areas of cyber- and IoT security. IoT cybersecurity incidents that were visible in the media, such as hacks of **Amazon**'s Ring cameras in late 2019, led to increased awareness of the need for better protection of IoT devices.

Correspondingly, a recent survey by IoT Analytics found that an overwhelming 83% of information technology professionals implemented stronger cyber hygiene among employees during the pandemic and plan to continue prioritising the subject after COVID-19. Other areas that saw significant increases in spending include cloud infrastructure for IoT deployments and IoT software applications.

This level of spending will need to increase in order to address the proliferating number of threats which are exacerbated by growing IoT device shipments. Internet of Things connections are expected to exceed 23 billion across all major IoT markets by 2026, according to **ABI Research**. The analyst firm's 'Device Authentication in IoT Technology' report reveals almost all those connections will be faced with incessant and constantly evolving cyberthreats, forcing implementers and IoT vendors to embrace new types of security to protect managed fleets and connected assets. Secure device authentication is among the top-tier investment priorities for key IoT markets, the firm reports. It expects that hardware-focused IoT authentication services will reach US$8.4bn in revenues by 2026. ▶



While these security gaps present a significant challenge for companies and end-users, they also represent a substantial opportunity for players in the IoT market, including IoT service providers, vendors, platform operators and and information technology (IT)/operational technology (OT) security organisations.

IoT organisations therefore need to prioritise addressing their greatest risks and find rapid and cost effective ways to protect themselves and users. The IoT skills gap means most organisations will turn to the IoT ecosystem to find ways to achieve more secure deployments that meet their cost and time constraints.

The main threats include:

- Lack of physical hardening of IoT devices
- Insecure data storage and transfer
- Weak passwords
- Insecure ecosystem interfaces
- Botnet attacks
- AI-based attacks
- Weak device management

Botnets, advanced persistent threats, distributed denial of service (DDoS) attacks, identity theft, data theft, man-in-the-middle attacks and social engineering attacks are the main crimes that target IoT but this is not an exclusive list. The steep growth in new IoT connections over the next five years with increased digitisation and automation across many different industries will see greater need for IoT security but ABI Research points out the amount of IoT security revenue does not always correlate with the amount of IoT connections, and some markets are expected to experience disproportional revenue.

The increasingly rich functionality and capability that connected devices are assembling and are set to derive substantial value from increases the security risks. **Transforma Insights** has reported cloud and edge computing, machine learning, mobile private networks and 5G are just a few examples of richer functionality being applied to IoT and these are enabling enterprises to use IoT for more critical systems, with the consequent requirement for more sophisticated features and capabilities, and, of course, more robust security.

At the same time the firm says an almost contradictory trend is occurring. IoT technologies are being rapidly refined to support applications deployed in highly constrained environments. Large volumes of connections must cope with limitations on, for instance, access to power, physical and cost limitations on componentry, and geographical remoteness limiting availability of networks. Transforma Insights refers to these constraints as the five Ps: power, processing, place, price and proportions.

The key to overcoming these constraints is in delivering what Transforma Insights terms Thin IoT. This consists of deploying an optimum set of technologies across each of the five layers layers that make up a solution: device hardware, device software, networking, middleware, and edge computing and machine learning. These include system-on-chip, chip-on-board, embedded operating systems such as TinyOS and RIOT, networking technologies such as message queuing telemetry transport (MQTT), constrained application protocol (CoAP), and low power wide area (LPWA) technologies, thin middleware, and data processing techniques such as tiny machine learning (TinyML).

Secured via the SIM

IoT device connectivity is becoming more secure, ensuring the identity of the device is better protected than using a traditional plastic SIM card. New SIM technologies such as embedded SIM (eSIM) and integrated SIM (iSIM) have the potential to ▶

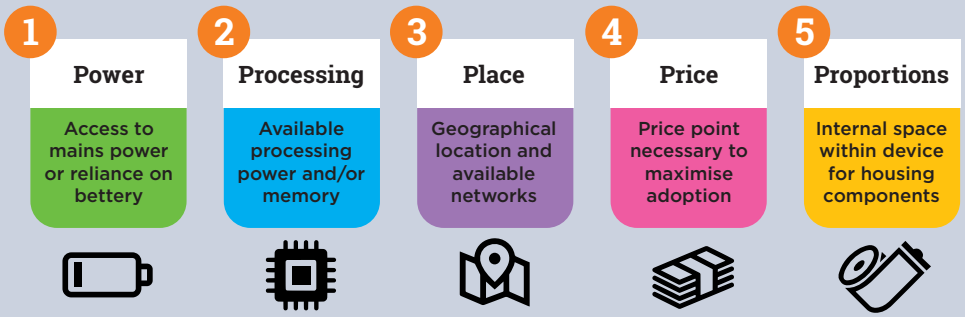


Figure 2: The five Ps that constrain IoT

Source: Transforma Insights, 2021

offer improved security but adoption is at an early stage and there are challenges to be addressed regarding secure key sharing between network operators.

The embedded universal integrated circuit card (eUICC) should remove the need for physical sockets in devices which can be a point of criminal ingress and the capability to manage embedded or integrated SIMs remotely via remote SIM management systems. These systems or platforms provide users with a fully-tested means to provision secure connectivity and protect the device identity.

The physical machine form factor (MFF2) embedded SIM has been available since 2016 and the ability for remote SIM provisioning (RSP) for several years before that, finally being standardised in 2016. Since then, the integrated SIM (iSIM) arrived in 2018 moving the SIM functionality to a secure location on silicon along with the application processor and radio, all implemented on the same system-on-a-chip hardware.

Beyond the pandemic

With cybercrime increasingly professionalised and state actors targeting enterprises, IT security in general is a priority and IoT security in particular is being seen as an important subset of that. Organisations now understand the threat surface is radically enlarged by IoT devices and the consequences of a breach can be catastrophic. The challenge is to secure IoT in a way that lower value applications can afford.

Innovations such as eSIM and iSIM allow improved security to be installed at the point of manufacture and reduce frauds and crimes associated with localised configuration and traditional plastic SIMs. However, there is still work to be done in defining how SIM security will be maintained and managed.

Inevitably secure connectivity enabled by secure SIM technology does not comprehensively address the security challenge. At every stage of the business chain, security must be prioritised to protect users, data and the enterprise. However, as is typical with all technology, the point at which a secure architecture touches a human is often its weakest. IoT must therefore adopt the latest innovations in security to protect itself but it must also focus on the fundamentals of strengthening passwords, controlling identity and access management and addressing the easy wins of hardening IoT devices.

INTELLIGENT IOT CONNECTIVITY

Advance IoT with Us

The **Aeris Intelligent IoT Network** is the only cellular network built from the ground up with **intelligence** at its core. It offers superior connectivity, security, performance, visibility and best-in-class support across IoT deployments.

With Aeris, our clients can bring solutions to market quickly, scale deployments effectively, and expand globally—all while maximizing value from connected solutions.

aeris®

Learn more at:
info.aeris.com/intelligentIoT