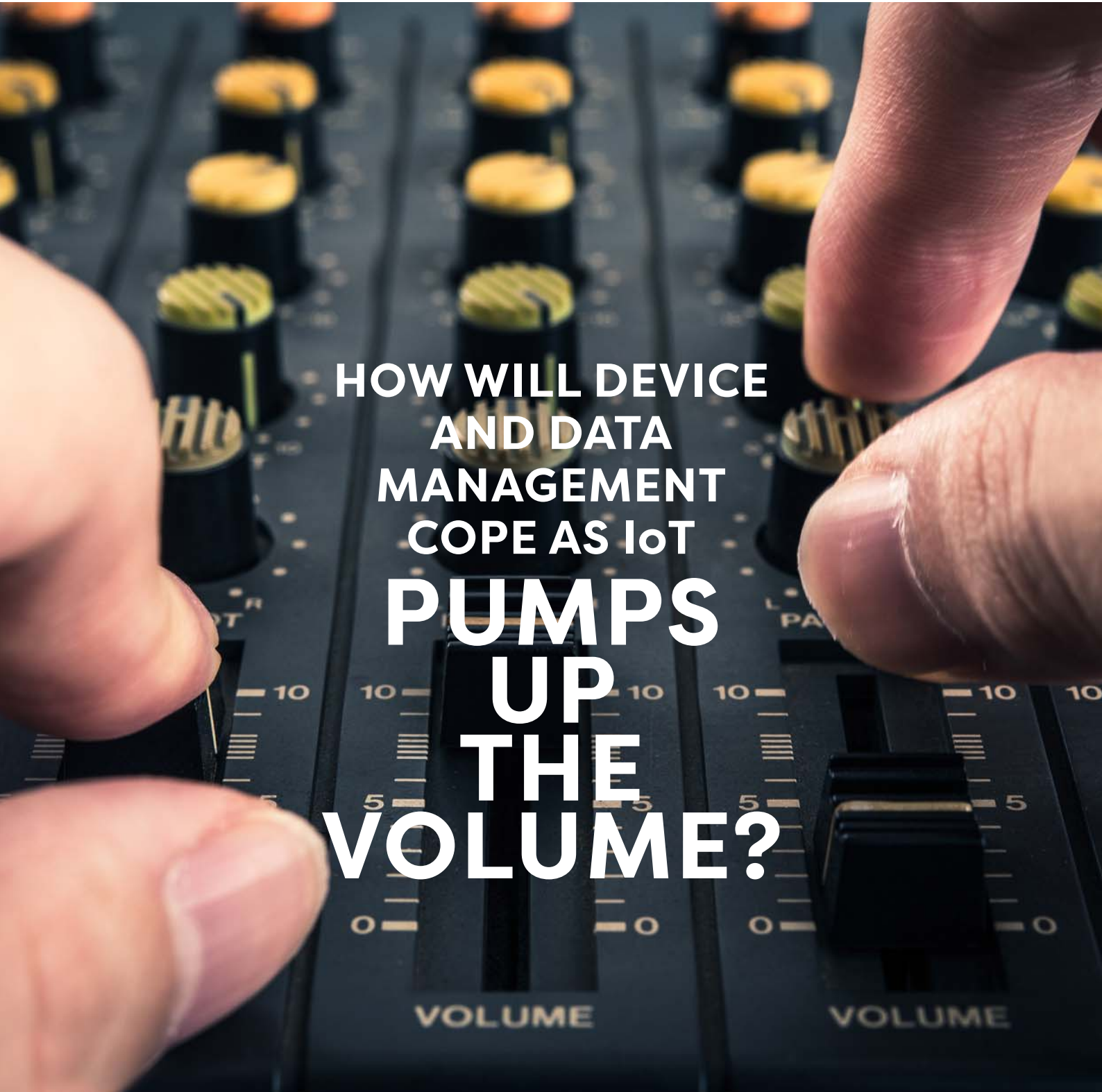


IoT tech trends

Your inside track on the technology topics that matter



HOW WILL DEVICE
AND DATA
MANAGEMENT
COPE AS IoT
**PUMPS
UP
THE
VOLUME?**

Vol. 1, No. 2

Value per report £99 but **FREE** for anyone that registers to
IoT Global Network www.iotglobalnetwork.com

Secure management of IoT devices at scale

Any Device | Any Vendor | Any Network | Any Cloud

Onboard, manage, update and secure scalable deployments of IoT devices using a flexible SaaS to deliver on the promise of IoT-enabled business.

arm.com/device-management

arm PELION

Editor's overview



04
IoT devices set the challenge of data with destiny

The numbers in terms of new devices to connect and the volume of the data they will generate are massive, reports **George Malim**. The next IoT challenge therefore becomes managing devices and the data they create to generate valuable insights.

Device Security



16
Why a trusted device equals trusted data
Security starts even before establishing the root of trust to secure devices and the data they generate, store and transmit from the chip right through to data hitting the cloud, writes **Annie Turner**.

News



06
A round up of the latest IoT device and data management news

Cloud vs On-Prem



20
Should you manage your device data on the cloud or on your premises?
Advocates for managing the information in-house have lost their majority in a massive swing in consensus. The conventional wisdom about cloud management has changed from why to why not, writes **Nick Booth**.

Analyst report



08
How to prepare device management for hyperscale in IoT
Organisations making IoT deployments have to prepare in terms of device and data management if they are to succeed in the mass IoT market, writes Beecham Research's **Robin Duke-Woolley**.

Device Lifecycle Management



22
Good device management can underpin successful data strategies
Potentially billions of IoT devices have to be securely deployed and managed from the chip right through to the data, whether that's on-premise, at the edge or in the cloud. **Antony Savvas** explores device management throughout the device lifecycle.

Sponsored interview



12
Data volume and variety makes device management vital for efficient IoT data processing
Hima Mukkamala, the senior vice president and general manager of IoT Cloud Services at Arm, tells **George Malim** that device management is critical for organisations that deploy IoT devices, collect their data on-premises or in the cloud, and analyse it for business use.

Device Data



24
Device data demands management strategy and automation at hyperscale
If there are billions of devices there will be trillions of data points transmitted on an often-daily basis. **George Malim** examines how all of this will be managed from the chip on the device through to the cloud, edge or on-premise data processing capability.

IoT Global Network tech trends covers technological & business developments for businesses enabled by the Internet of Things (IoT). © Copyright WKM Ltd. All rights reserved. No part of this publication may be copied, stored, published or in any way reproduced without the prior written consent of the Publisher.

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

Business development:
Cherisse Jameson
Tel: +44 7950 279368
c.jameson@wkm-global.com

Designer:
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



IoT DEVICES SET THE CHALLENGE OF DATA WITH DESTINY

The numbers in terms of new devices to connect to IoT and the volume of the data they will generate are massive but only parts of the data and the insights held within it are valuable. The next IoT challenge therefore becomes managing devices and the data they create to generate valuable insights without the costs running away with themselves, writes George Malim.

Analyst firm **Gartner** has reported that it expects the number of internet-connected devices to hit 5.8 billion by 2020, with growth set to continue at a rate of 20% year-on-year. Data from **IoT Analytics** says there are currently about seven billion IoT devices and projections and estimates generally put IoT device numbers in the single-digit billions. This is far from the numbers of devices suggested at the peak of IoT's hypecycle five years ago, which talked in terms of 50 billion devices by 2020, but it's still a large number and evidence is starting to show huge volumes of device additions per month.

In the mid to long-term it won't matter that the 50 billion connections weren't made next year. That apparent failure is only

a symptom of overhype that all new technologies are subjected to. The missed projection will pale into insignificance when the real volumes arrive. Research from **Arm**, for example, estimates one trillion devices by 2035.

I think everyone gets it now that IoT is here, it's growing and it will stay and become central to our existences, our businesses, our jobs and our families. However, all of these devices – whether they're disposable adhesive labels being used to track parcels or industrial machines with expected 40-year lifespans – will need to, as a minimum, collect and communicate data. Some will apply intelligence to that data, reducing the need to communicate data or to process it in the cloud because that can be performed locally ►



George Malim

Tech Trends

by a more intelligent device. Others will be simple, dumb and cheap existing only to say the rubbish needs collecting or the fluid is leaking.

Think of, say, ten billion devices pinging small data points every hour, which is not unrealistic within the next five years, and then add to that a few billion more sensitive and intelligent devices that need to almost continuously stream highly detailed performance data and suddenly we're in a world of data that hasn't been seen before, even in the wildest dreams of 8k video multi-player game streaming enthusiasts.

The scale is simply enormous. Research firm **IDC** expects worldwide data to hit 175 zettabytes by 2025, an increase from 33 zettabytes last year, and of that, 90 zettabytes will be created by IoT devices by 2025. I had to look up what comes next after zettabytes. It's a yottabyte and it's looking more and more likely we'll see data hit a yottabyte during readers' lifetimes.

But what does all this data mean? As Peter Ruffley points out on page 24, much of it will be completely worthless and simply clog up storage and networks, waste analytical resources and cost money unnecessarily. There's a perception that being able to aggregate data from disparate resources will suddenly make it valuable and this may prove to be true but today we just can't tell.

Will a cleaning company's sensors that help it decide how often to clean a bathroom be able to share data with building owners to allow them to more accurately control cooling and heating in less-heavily occupied parts of the building? Will HVAC data combine with cleaning company data plus hot desking bookings to enable companies to rent smaller offices or urban authorities to plan for reduced commuter traffic on public transport? Perhaps, but aggregating and integrating all of these data points from disparate systems, owned by distinct and possibly competing organisations seems many years away and, in fact, so far away as to be unrealistic for today's deployers of IoT.

Important questions remain to be answered about why a building owner would want to share data with a tenant that could cause them to rent less office space. And this goes without considering how data could be sanitised and shared securely between organisations and how company A could be compensated by company B for the shared insights.

This may be where we're going but it's too early to tell and organisations clinging on to data simply in the hope that it will be useful in future maybe investing in a data storage facility that turns out to be full of junk. Nevertheless, there are also zettabytes of useful data being generated in IoT today and that's where the immediate value lies that will justify continued investment and roll-out of IoT technologies. This may be happening in isolation – the cleaning company knowing a bin needs emptying is useful and extrapolating that to enable a predictive pattern so it knows when to schedule bin emptying makes the business case for a simple connected sensor, for example – but the next step becomes more complex.

Added to this need to handle data outside of traditional siloes and across multiple different formats and platforms, is the proliferation of the devices themselves. Gartner has estimated that by 2023, the average CIO will be responsible for more than three times the number of endpoints they managed in 2018. That's a huge uplift and will require focus on security, uptime, maintenance and cost, all of which will need to be balanced against the reward that these devices provide. The reward might be new revenue but it could be greater operational efficiency or employee satisfaction.

As is so often the case in IoT, the opportunities are endless. This issue of **Tech Trends** therefore is focused on the challenges of managing devices and their data at hyperscale. The whole picture isn't clear yet but it is more than apparent that the foundational platform of hyperscale device and data management is a prerequisite for success as IoT changes gear and charges into the next phase of its growth. ■■

Increasing penetration of IoT-based devices boosts popularity of location-based ambient intelligence

The global location-based ambient intelligence market is projected to reach a value of approximately US\$497bn by 2027, according to a new report from **Transparency Market Research**. The firm says the market is projected to expand at a compound annual growth rate (CAGR) of about 21% from 2019 to 2027.

Growth of the location-based ambient intelligence market can be attributed to the rising demand for energy-efficient solutions, globally. Over the forecast period, the Asia Pacific region is anticipated to grow rapidly at a CAGR of approximately 25%.

In terms of market share, the location-based ambient intelligence market is dominated by North America, followed by Europe. In the location-based ambient intelligence market, the smart homes segment was valued at approximately US\$42bn in 2018, and is expected to reach approximately US\$200bn by 2027, expanding at a CAGR of approximately 19% during the forecast period.

Increased advancements in IoT are expected to boost the demand for smart homes, globally, during the forecast period. Decline in the price of processors and sensors and greater networking capabilities, coupled with extensive Wi-Fi access, have fuelled the expansion. Smart home systems are growing with the introduction of high-speed internet services, since a majority of appliances operate efficiently with wireless connectivity. The extensive usage of Wi-Fi in residences is boosting the location-based ambient intelligence market, as several appliances can be connected to the home network without the use of additional controllers.

Casio selects secured platform to protect smartwatch data

Device and application security provider **Trustonic** reports that **Casio** has selected its Trustonic Secured Platform (TSP) to bring additional security and trust to its new watch, the Casio PRO TREK Smart WSD-F21HR. Launched in August, the watch includes GPS, offline maps, heart rate and VO2 max measurement.

Casio will use Trustonic's hardware-backed security to enable enhanced smartwatch features, functionality, speed and ease of use for outdoor adventurers. Trustonic is helping Casio to protect the sensitive tracking and biometric data that is now stored and transmitted by wearables.

"Wearables are rapidly gaining momentum, driven by consumer demand for cool, new features and richer experiences," said Ben Cade, the chief executive of Trustonic. "To future-proof

smartwatches, deliver new functionality and safeguard the personal data captured, processed and transmitted by them, innovative OEMs like Casio are looking to the security best-practices of the smartphone ecosystem. Our TSP platform

enables devices to be designed, developed and built on a proven foundation of hardware-backed trust."

TSP is already deployed in two billion smart devices and protects connected devices such as wearables, smartphones, automotive in-vehicle infotainment (IVI) platforms and healthcare devices by delivering industry-standard based, hardware-backed security.



Casio's PRO TREK Smart WSD-F21HR

Arm announces Custom Instructions for embedded CPUs and Mbed OS Partner Governance

Simon Segars,
Arm



Arm CEO, Simon Segars has announced Arm Custom Instructions, a new feature for the Armv8-M architecture.

Arm Custom Instructions will initially be implemented in Arm Cortex-M33 CPUs starting in the first half of 2020 at no additional cost to new and existing licensees, enabling SoC designers to add their own instructions for specific embedded and Internet of Things (IoT) applications without risk of software fragmentation.

In addition, Arm is moving to a new

Mbed OS Partner Governance model, where its silicon partners can directly influence future development and enhance the company's efforts in building out new capabilities, features and functionality for its Mbed OS free open-source operating system. Any Mbed Silicon Partner Program member is welcome to join at no cost. Several of Arm's silicon partners including **Analog Devices, Cypress, Maxim Integrated, Nuvoton, NXP, Renesas, Realtek, Samsung, Silicon Labs** and **u-blox** are already actively participating in the working group.

Monitored alarm systems in Europe and North America hit 46m at the end of 2018



Martin Bäckman, Berg Insight

Berg Insight, an M2M/IoT market research provider, has released new findings about the market for connected security applications. The number of monitored alarm systems in Europe is forecast to grow from 15.6 million in 2018 at a compound annual growth rate (CAGR) of 3.6% to reach 18.6 million in 2023. In North America, the number of monitored alarm systems is forecast to grow at a CAGR of 2.9% from 30.7 million at the end of 2018 to 35.4 million at the end of 2023.

Small alarm systems for businesses and private homes can be divided into two main categories – local alarms and monitored alarms.

There is still significant growth potential for monitored small alarm systems, especially in Europe where the total penetration reached only 6.4% of all businesses and households at the end of 2018.

"The penetration of monitored alarm systems in North America is much higher than in Europe and the corresponding figure in this region was 23% at the end of 2018," said Martin Bäckman, an IoT analyst at Berg Insight.

"Alarm systems are becoming more valuable for customers as the scope of offerings are being expanded to include detection of fire, carbon monoxide and water leaks, as well as home automation features."

Transformative urban digital twin and city modelling deployments to exceed 500 by 2025, says ABI Research

The digital twin concept and the urban modelling paradigm, more generally, are transforming how cities are designed, monitored and managed. They allow optimising of the holistic performance of cities across verticals in terms of energy management, mobility, resilience, sustainability and economic growth.

Digital twins combine spatial modelling of the urban built environment, modelling of electrical and mechanical systems based on mathematical descriptions or deep learning informed training and real-time sensor data derived from IoT platform solutions. The installed base of deployments is expected to grow from just a handful of early implementations in 2019 to more than 500 by 2025, according to global tech market advisory firm, **ABI Research**.

"Originally developed for industrial systems, the digital twin concept is now spreading to the smart cities environment," said Dominique Bonte, vice president and markets at ABI Research. "However, it won't be a single **Uber**-like digital twin for an entire city but rather an aggregation and integration of domain-specific digital twins for systems like smart buildings, traffic infrastructure, energy grids and water management."

Key use cases across verticals include the simulation of people movements and emergency evacuations, modelling of flooding risks, smart building design and

energy management via occupancy tracking, road traffic modelling and simulation, air quality monitoring and prediction, modelling of green infrastructure and circular urban economies, and cyber threat analysis.

The benefits of modelling are numerous and range from preventive maintenance to operational efficiencies and cost savings, improved services for citizens, increased safety and security and the inherent possibility of automated generative design, for example allowing maximising solar energy exposure of entire neighbourhoods.

However, challenges for adoption remain, mainly related to the complexity of city-wide modelling and the lack of standards supporting cross-vertical data exchange. Other inhibitors include the little awareness about benefits and ROI, commercialisation challenges related to the siloed organisation structure of city governments, and concerns about consumer privacy and cyber threats.

In spite of the challenges, it is quite clear urban modelling and digital twins, in particular, form the end game of the smart cities journey to optimised design and the ultra-efficient operation of entire cities. "Just adding a thin layer of IoT tech on top of legacy infrastructure will no longer suffice to address the multiple challenges cities will face in the future," Bonte added.

New database aims to enhance resilience, performance, interoperability, compliance and security for IoT

Crate.io, the developer and supplier of the CrateDB IoT-optimised database technology, has released CrateDB 4.0. With updates that address several components of the highly scalable open source database, version 4.0 is said to make it easier, faster and more cost-effective for IoT- and IIoT-fuelled organisations to put their machine and sensor data to work.

CrateDB is a distributed SQL database based on a NoSQL architecture that takes advantage of the convenience of SQL for processing any structured or unstructured data type. Dynamic schemas make it extremely easy to add new data types or indexes, and the architecture allows horizontal scaling by interconnecting servers to capture millions of IoT and IIoT

data inputs per second – totalling hundreds of terabytes in cluster size. Distributed processing, data partitioning, and in-memory indexes return millisecond responses to time-series requests – even when many clients are working in the database simultaneously.

CrateDB has been deployed by organisations where vast amounts of sensor and machine data in a variety of formats need to be instantly and continually captured, stored and analysed. Deployed and trusted by large enterprises including **Nokia**, **Gantner Instruments**, **Qualtrics**, **Comcast** and **ALPLA**, CrateDB handles millions of data points per second with fast, linearly-scalable data ingestion.

IoT Global Network

IoT tech trends REPORT

Although later than projected, IoT connections are finally starting to ramp up in volume as the IoT industry moves from trials and pilots to real world deployments at scale. However, the proliferation of connections is only one part of an IoT solution. Alongside huge numbers of connections come huge numbers of IoT devices and these devices will generate data at hyperscale. Organisations making IoT deployments therefore have to prepare in terms of device and data management if they are to succeed in the mass IoT market.

HOW TO PREPARE DEVICE MANAGEMENT FOR HYPERSCALE IN IoT



Robin Duke-Woolley

CEO

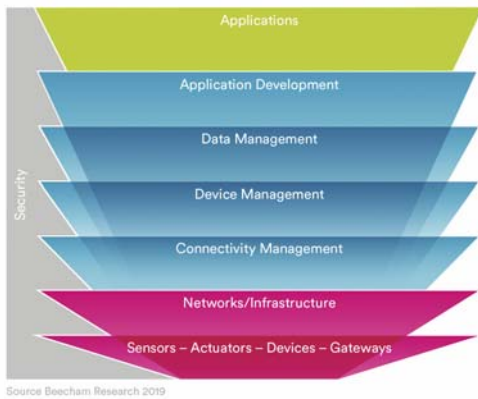
Beecham Research

Elements of an IoT solution

For any IoT solution involving connected devices, there are three key elements that must be managed:

1. **The connected device**, that may be one sensor measuring temperature, location or some other parameter or an asset such as a vehicle that has many sensors each measuring something different. Device management aspects may include device identity in the network, provisioning for use of the network and secure over-the-air update of device firmware. These and other related areas are part of Device Management.
2. **The connection**, from the device to a server to which the data is transmitted for processing. That may be a short-range or long-range connection, wired or wireless, or a combination thereof. The server may be at the network edge or in the cloud, or in both for different needs. Some of the areas that need managing are connectivity options, coverage, network protocol support and billing/usage. These and other related areas are part of Connectivity Management. ►

Figure 1: Elements of an IoT solution



3. **The data** generated needs to be stored, processed – sometimes in real time – either on its own or in combination with other data, to create results. Additional areas that need managing are: workflow handling, visualisation, orchestration and data analytics. These and other related areas are part of Data Management.

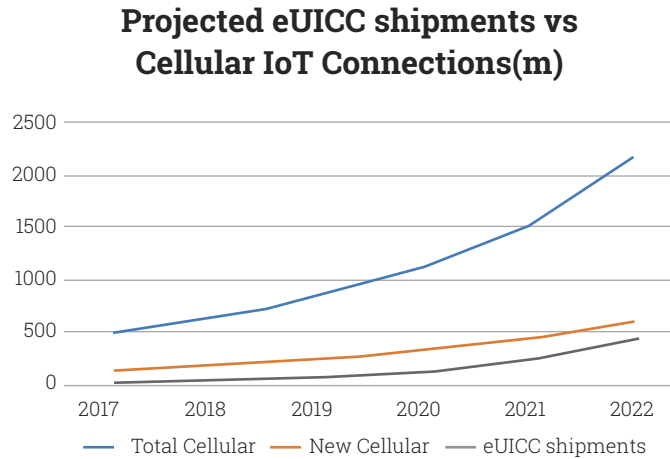
In addition to these, an application usually needs to be developed or provided to make specific use of the data created. All of this must be carried out securely so that the device itself and anything that is using the data, such as a controller, is not compromised. Security needs to bind together all the other elements so that potential attack surfaces are minimised.

These elements can be illustrated as in **Figure 1**, where they form a stack that sits above the sensors and network infrastructure. Since Device Management requires the connectivity to be in place before it can function for remote devices, it sits above Connectivity Management.

These are then also the main elements of an IoT platform, which is essentially a software middleware suite that facilitates secure monitoring, control and analysis of device and sensor behaviour in the field. In essence, it provides an enabling layer between these connected devices or sensors and user applications.

IoT platforms have been created for the express purpose of reducing the time and cost of getting new IoT solutions built and implemented. As shown in Figure 1, there are several layers to an IoT solution and these are becoming increasingly complex as the market develops. The IoT platform takes advantage of the fact that the majority of what is needed in IoT solutions is the same and does not need to

Figure 2: Cellular IoT market growth



be redeveloped for every application. In theory, at least 80% of IoT solutions are made from common parts, so can be pre-designed and made available through an IoT platform. The platform then also provides the means for customising and configuring the solution (the other 20%) for a specific application need.

To some extent, this is why there are so many IoT platforms on the market – well over 500 at this time. Some have a narrow market focus and specialise in particular application areas – such as smart city or smart energy – while others provide a more horizontal capability that aims to satisfy requirements across a wider range of vertical sectors. In reality, what has been found is that those with a narrow market focus typically have less customisation to do for any one project (more like 90%:10% rather than 80%:20%). On the other hand, those with a more horizontal platform often find more customisation is required (more like 70%: 30%). Either approach is still far preferable to building a new platform from scratch for each new IoT solution required.

Towards hyperscale – new challenges for IoT platforms

Preparing for scale is a huge challenge for IoT, and for IoT platforms in particular. While there are many IoT forecasts currently being talked about, some more optimistic than others, the general consensus is for rapid growth over the next decade.

Figure 2 shows expected growth for cellular IoT connections to 2022 at an overall rate per annum of 35%. This is aided by the introduction of new cellular technologies LTE-M and NB-IoT specifically for IoT at the lower data rate end of the market. Yet within this growth is an even faster change, which is the growth in use of embedded SIM (eSIM) solutions and associated embedded universal integrated circuit cards (eUICC). The eUICC is expected to feature in a growing proportion of new cellular IoT connections, so that by 2022 up to 67% of new cellular IoT connections will be eSIM based. At that rate, eSIM – and in the future integrated SIM (iSIM) – will become the new norm for cellular IoT. This change represents a substantial challenge for IoT platforms to cater for over the next few years.

Beyond cellular, other technologies like Bluetooth and Wi-Fi are also set for increasing IoT use, with the number of such short-range connections in the orbit of 8x cellular connections by 2022. Overall, this means that IoT connections are likely to exceed 15 billion by that time. This represents a further huge scalability challenge for IoT platforms.

While these changes are developing, for an increasing number of businesses IoT is rapidly moving from nice-to-have to strategic necessity. At its simplest, an IoT solution provides the opportunity to save operational costs, introduce new service revenue opportunities, or help to ensure compliance with new regulations. In practice, it is increasingly a combination of these dressed up in a wide range of ▶

Figure 3: Arm's Pelion IoT Framework

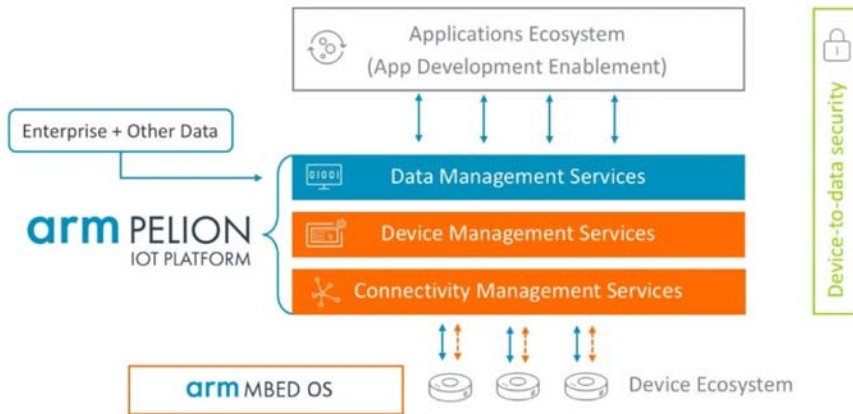
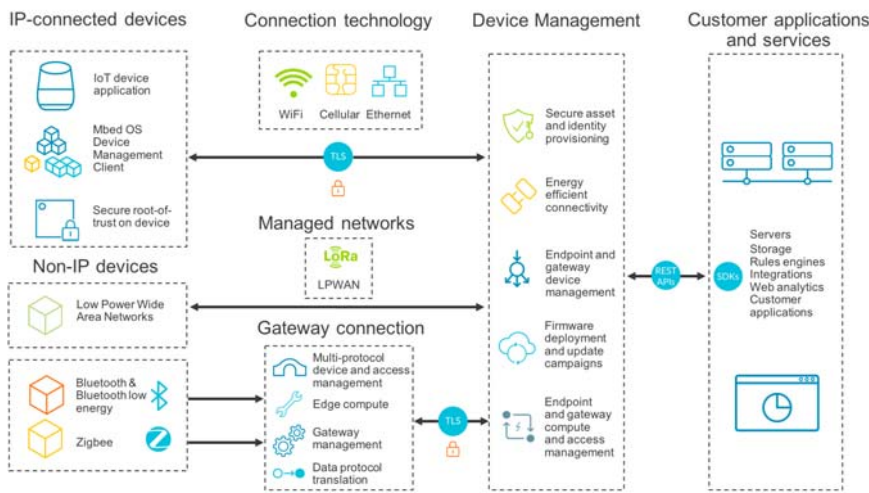


Figure 4: Pelion Device Management



business needs, some more urgent than others. It gets more challenging when that means processing large amounts of data in real-time to support current business operations. It can be more challenging still to integrate these new real time data flows with traditional batch update data typical of IT systems already in use. Those challenges increase yet further when these data flows need to interoperate smoothly and securely across several different business operations, all in real-time.

To cater for these and other challenges and create an IoT solution that will stand the test of time, IoT platforms must adapt further. Yet all of this needs to be managed within a secure environment. There is no doubt that, over the next few years, there will be increasing reliance on the huge amounts of data collected through IoT solutions. So long as we can trust it, this data will become relied on by all of us, driving business insights and transformations everywhere. This trust is all-important. If

we are going to depend on this device data, we need to be sure it is genuine. That means having the right level of security for each use case, which in turn requires a framework to be in place for securing large numbers of connected devices.

Arm's approach to IoT

Figure 3 shows the main elements in Arm's Pelion IoT Framework, including the Pelion IoT platform. This follows directly the principles outlined in Figure 1.

In addition to the Pelion IoT platform layers, Mbed OS is a free, open-source embedded operating system that comprises of all the necessary features to facilitate the development of IoT connected products, including standards based security and connectivity stacks, an RTOS kernel, middleware for storage, and networking, and remote device management. It is particularly suitable for small, constrained devices with limited processing and storage and

integrates closely with Pelion Device Management in particular. Also, of note is Arm's Platform Security Architecture (PSA), a framework that ensures secure IoT devices with Root of Trust. When coupled with Pelion IoT Platform services' security features like Trusted Boot and Firmware Update, data encryption, and developer application programme interfaces (APIs), PSA provides an end-to-end security solution.

With 95% of the world's smartphones based on Arm and over 150 billion Arm-based chips shipped to date, Arm is already very familiar with the challenges of scalability. This experience has been incorporated into the Pelion IoT platform layers, including Pelion Device Management. This layer is expanded in Figure 4.

The rapid growth of connected devices expected in the IoT market over the next decade presents major challenges for device management. The mix of such devices will include both highly constrained devices with limited on-board power, storage and processing capabilities, to fully featured end nodes and gateways. All of these will require secure remote management. In addition, information requirements from device data is increasing quickly, with greater use of analytics, visualisation tools and – as these mature – greater use of artificial intelligence. This means vastly more traffic utilising a wider variety of data processing resources, with increasing opportunities for that data to be compromised. This requires a robust chip-to-cloud approach for security. Pelion Device Management, coupled with PSA, enables secure and reliable onboarding, monitoring, updates and lifecycle management of the wide mix of types of connected devices expected in the future.

Examples of Pelion in action

1. Bringing connectivity, scalability and security to constrained devices

The challenge: A global manufacturer of high-end consumer embedded devices undertook a review of their product portfolio after a number of successful iterations of their product. Their custom-built hardware solution is paired with their scientifically-researched algorithm, which generates user data in real-time on the device. Market success has meant that the algorithm has become the subject of much

competitor interest. They concluded that additional security measures to protect their intellectual property would be critical to maintaining their differentiation and market share.

Hardware constraints within the existing product meant incorporating additional measures to existing devices would not be simple. They realised they would need a partner to guide them with best practice advice and help them build a whole new software solution with additional capabilities within the constraints of existing hardware.

The solution: Arm's comprehensive knowledge of software development for embedded devices, combined with the capabilities of the Pelion IoT platform and Mbed OS enabled them to overcome these challenges.

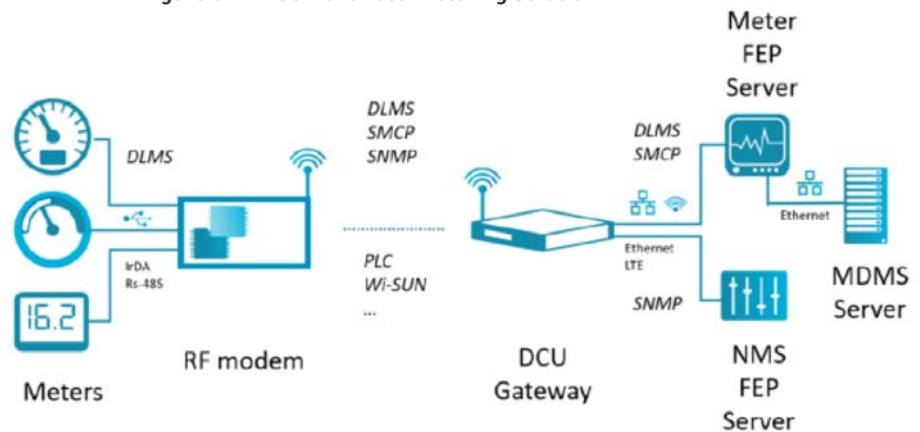
The solution bolstered the feature set of their constrained devices, including adding a complete operating system to the device firmware; chip-to-cloud encryption and communications protocols to protect user data; and numerous specific defences against hardware attacks on the device to detect and report attacks to the enterprise's security operations centre.

After their initial market success, the projections for the ramp up of device production meant they needed an IoT device management platform that could scale with their ambitions. Pelion Device Management handles automated monitoring, support and update for many millions of intermittently connected devices, whilst Mbed OS provided a foundation for the IoT platform. Together with Arm, they also needed to go further to build and integrate the solution with their existing digital services.

2. KEPCO Advanced Metering Infrastructure

Korea's sole energy provider Korea Electric Power Company (**KEPCO**) was embarking on a digital IoT transformation that helped facilitate their transition from an energy provider to an energy platform and service company. This evolution involved complementing their infrastructure with 30 million smart meters and deploying an additional billion IoT nodes across their very large grid.

Figure 5: KEPCO Advanced Metering Solution



However, the challenges faced by KEPCO were numerous and included concerns over:

- Device security
- Lifecycle management of deployments on a very large scale
- Wireless connectivity
- Real-time billing data collection

KEPCO chose Arm's Pelion IoT platform as it could provide a dedicated chip with end-to-end security complemented by an IoT operating system (OS), device management tools, hardware IP and consultancy services. Arm was tasked with two key objectives:

Objective 1 – Device control: Arm's Internet Services Group (ISG) offered the means to securely manage devices' on-boarding, monitoring and updating, and even decommissioning of the device at the end of its lifecycle. Over the Air (OTA) updates mean additional security patches and functionality can be administered without the need to physically travel to support remote devices.

Objective 2 – Chip-to-cloud security and efficiency: KEPCO utilised both Arm's ISG support and IPG's (IP Products Group) secure chipset to reduce time to market, also creating a solution to ensure these insights are shared with partners and customers easily and securely. Come 2021, Pelion Device Management will be responsible for the onboarding, connecting and updating of both devices on a national scale. The platform will consolidate a very large number of data feeds and manage devices via a single pane of glass, as well as simplifying and securing the management of each stage of the device's lifecycle. This includes managing data indicating device health and billing, relayed to KEPCO in real-time. This information is then also shared via APIs to their partners and bills to customers.

KEPCO engaged with several original equipment manufacturers (OEMs) to help deliver the very large number of meters required. Third parties used Arm's Mbed OS and toolchain, including Mbed Studio, Mbed CLI and Manifest Tool. These applications are part of a suite of tools and reference designs created to expedite application development, debugging and web services integration. Arm's Pelion IoT platform supports a broad range of connectivity options, meaning meters and gateways could communicate via the low energy, low latency qualities offered by WiSUN wireless communications, before relaying to KEPCO's on-premise servers.

Arm collaborated with KEPCO's joint R&D partner **ARGO** to create a custom System on Chip (SoC) powered by a Cortex-M3 for meters and with OEMs for a highly secure KEPCO gateway infrastructure powered by an Arm Cortex-A9 and Arm TrustZone. This collaboration, combined with a suite of tools, are helping KEPCO to trial, then mass deploy gateways and millions of smart meters by June 2021. ■■

To read the full KEPCO case study visit <https://learn.arm.com/kepcO-iot-case-study>

DATA VOLUME AND VARIETY MAKES DEVICE MANAGEMENT VITAL FOR ENSURING SECURE, EFFICIENT IoT DATA PROCESSING

Hima Mukkamala, the senior vice president and general manager of IoT Cloud Services at Arm, tells George Malim that device management is critical for organisations that deploy IoT devices, collect their data on-premises or in the cloud, and analyse it for business use. However, as device volumes increase and the sheer diversity of IoT applications and devices fragments the landscape, IoT device management is becoming far more complex than the traditional discipline of enterprise IT device management. What's needed are a set of tools, processes and disciplines to manage the volume and variety, while also ensuring ease of use, validity of data and security.

George Malim: We've all seen the projections of IoT hitting hyperscale in a very short time from now and this has an obvious impact on the number of devices that organisations will need to manage. What do you see as the challenges of managing the sheer volume of devices?

Hima Mukkamala: I think that the volumes to date haven't gone quite as projected, but we're starting to see IoT hit that inflection point that the industry

has been talking about, as organisations are beginning to obtain value from IoT. There are definitely challenges - including the diversity of devices and use cases, security concerns and complexity - that have held back some of the growth.

Every use case places a specific requirement on the IoT device and the network, which can make scaling difficult. On the security side, there's a lot ▶

more visibility into and awareness of the issues, but the challenge is in making sure devices and data are secured throughout the device lifecycle journey, especially as organisations add more infrastructure and solutions to their environment, such as moving data to the cloud, outside of it and at the edge.

Another important challenge is that, as more is added to existing workflows and processes, the landscape becomes more complex. That will continue as volume ramps up.

As many of the use cases start from the factory in siloed environments, it can often be difficult to change the devices later.

GM: Beyond management of the devices themselves, the next and probably greater challenge is managing the data the devices will generate. How can organisations put in place a successful strategy for device data management?

HM: When we talk about device data management, it's a combination of digital and physical device data. Physical data is the data coming from devices, but the outcomes that enterprises care about are achieved by combining this with their existing digital data so we need to look at solutions that can handle physical and digital data. Pure physical data gets siloed and doesn't deliver meaningful insights.

The second aspect of device data is that it should be trusted data. If data cannot be trusted there's a risk of generating wrong insights. Therefore, enterprises' should look for IoT solutions that include a means to ensure data is trusted.

With our Pelion Data Management we address how to bring all the heterogeneous sources of data together. This is important not only in combining physical and digital data, but also because deployments tend to be in brownfield situations where organisations need to manage existing devices in addition to new devices. Pelion Data Management also enables enterprises to obtain trusted data, as the data is encrypted both at rest and while in transit.

GM: For most organisations there won't be just one type of IoT device to manage so how will organisations

approach device management in a way that encompasses the diversity of devices involved?

HM: One of the successful strategies that has evolved in the market, especially covering brownfield environments, is the notion of putting a gateway in the middle so that old devices can be connected. Don't forget, in some industrial environments devices stay in place for 40 years and don't change.

In some cases, the volume of data is so great that it is not cost effective to send it all to the cloud. There is a trend towards using gateways in these deployments as well to enable a lot of the processing to be done in multiple layers –so some of the processing can be done in high-end cloud and data processing environments, while other processing can be done at the edge.

The aggregation point is starting to change. Enterprises want some of the devices to be managed on premises - i.e. without using a cloud. Also, the diversity means that customers don't want to deploy solutions that constrain them to a particular device. They want an operating environment that can manage any device, any network and any cloud.

GM: Where do you draw the line in Arm's characterisation of devices to be managed. Do you see system-on-chip (SoC), for example, as a form of device?

HM: Absolutely, we address a broad range of device types – ranging from ultra-constrained to full-featured – that may be powered by SoCs, low-power microcontrollers and others. We take a device agnostic approach to managing and updating all of these different devices. Also, while customers are deploying Arm-based devices, we recognise that not all devices will be Arm-based. We are able to support our customers with the solutions to manage any device, providing them with the flexibility that is needed to scale their IoT deployments.

In addition, one of the trends we're moving towards is integrated SIM (iSIM), where the SIM is built into the system-on-chip. This is the next evolution of eSIM, and both provide the ability to switch between networks. The value in iSIM and eSIM is that organisations can manufacture the device in one location and ship anywhere in the world, providing local connectivity. ►

“ We’re helping customers scale their IoT deployments to billions of devices through our Pelion IoT platform ”

Arm’s value in the market is in removing complexity and friction in how these devices are managed and connected. iSIM will bring innovation and freedom to integrate connectivity in to a broader range of devices.

GM: IoT device security is at the top of everyone’s mind and the risks seem well understood. How is Arm ensuring that its device management capabilities will perform the critical security roles required of them?

HM: We believe security is critical for IoT to scale, and Arm is providing device-to-data security through our intellectual property, Mbed OS IoT operating system, device management, connectivity management and data security capabilities.

Our Platform Security Architecture (PSA) initiative that we announced back in 2017 defined a framework to bring best practice approaches to IoT security. To expand upon that, we launched PSA Certified earlier this year, which delivers independent security testing, and trust to the market that devices are built securely from the ground up.

Our free open-source IoT operating system, Mbed OS, is also PSA Certified, and helps developers build IoT devices that have a secure foundation. Mbed OS is seamlessly integrated with our Pelion Device Management, which provides security from development to onboarding to management in the field to finally decommissioning the device.

Another critical capability from a device management perspective that we enable is secure over-the-air firmware updates for patching vulnerabilities and keeping devices up-to-date. This is critical as devices can be out in the field for several years, and it’s simply not feasible to manually update every single device.

The security for a consumer electronics device is different from a utility and so on and so forth. Our approach is to simplify the development and

management of devices and provide the security regardless of the customers’ requirements.

We are also complying with other certifications such as ISO27001 and SOC 2, which are important in securing the credentials as data moves from the device to the cloud.

Security isn’t just one initiative. It needs to be a combination of enterprise security, device security and network security.

GM: To what extent do you see device management as a security tool or discipline?

HM: There are a lot of parallels with the enterprise IT world and also in mobile. When we first started using laptops, they were new devices accessing the network, and there were no best practices for potentially installing or using untrusted applications. Over time, management tools came in to help mitigate some of these risk factors and make it more difficult to install things on your device.

However, things diverge in IoT. While endpoint management was easy from the enterprise perspective, in the case of IoT, device management can be challenging due to the diversity of devices from ultra-constrained to large gateways and everything in between. IoT device management is a critical part of maintaining the device lifecycle and enabling organisations to securely abstract insights from the data. It is also managing the app credentials and app provisioning in gateways, and needs to take into account how the device is onboarded and how it goes through manufacture to distribution and to the end user.

Overall, security is a big part in enabling the scale to reach the trillion devices that are expected by 2035, and device management will play an important role. Device management is both a discipline and a tool, the tools make sure the discipline can be performed effectively.

GM: The security of device data is of equal importance. How is Arm working to support this? ►



**Hima
Mukkamala**
Arm

HM: Looking back at the parallels between IoT device management and enterprise device management the goal is to create a trusted environment and to ensure the data within it can be trusted. Breaches in the chain of data can lead to untrusted data so data must be validated by working closely with data management technology to ensure it is uncompromised end-to-end, at rest and in motion.

Also, it's not just about the data. Organisations need to ensure that the right processes are in place so that only the right people within the organisation have access to the device. They can do this with solutions such as Pelion Device Management Secure Device Access.

GM: Please can you explain how Arm's Pelion Device Management has been designed to address the twin challenges of handling immense device volumes and the data they create?

HM: Fundamentally, if you look at the challenges associated with handling the volume of IoT devices and data, having scalable protocols is of immense importance. This is because organisations need to be able to move the right data without using a huge network footprint.

We're helping customers scale their IoT deployments to billions of devices through our Pelion IoT platform. On the pure device side, we're giving options to customers in terms of how they deploy infrastructure. This could be through highly available local clouds for organisations working with high volumes of device data. For example, a firmware update can be done intelligently, at the right time rather than swamping all devices when they're busy. We can also do delta uploads of specific parts of firmware to be updated rather than pushing to all. We additionally have Pelion Device Management Edge, a gateway solution that can help customers offload some of the scale and processes at the edge, so only some of the data is pushed into the cloud.

GM: How do you see the market developing between cloud-based and on-premises approaches. What do you see as the relative merits of each?

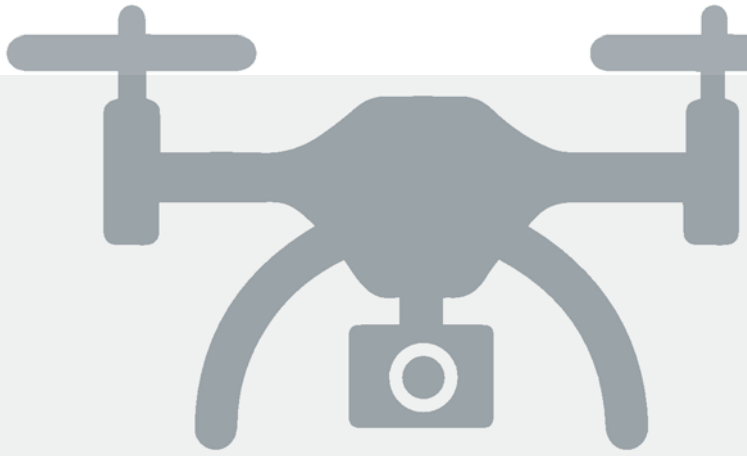
HM: It's an 'and' game. We will see a hybrid of cloud and on-premises approaches. Readily-available public cloud infrastructures have helped organisations deploy products quickly, reduce upfront capital costs and provide an excellent platform to test the waters and experiment on how a variety of different products and use cases could be brought to life on a small scale.

However, at least in some cases, when it comes to production-level deployments, on-premises option may be more suitable. For example, utilities use cases, often need to deploy in on-premises environments in order to comply with industry regulation. I think it's fair to say that this fragmented landscape, combined with bespoke use cases are emerging as areas where hybrid can solve the challenges associated with the abundance of devices that are arriving in deployments.

There are variations of these scenarios in virtually every customer deployment. That's why it's an 'and' game – each approach has its own benefits so, in general, the whole cloud compute market is adopting a hybrid approach.

GM: Is the need to scale-up stimulating interest in device management?

HM: The need to manage a large number of devices does stimulate the interest in device management. Every IoT device is managed by the appropriate service. Managing a small deployment of devices with little or no security is simple, managing a large number of devices with robust security from the production line and throughout the device lifecycle with secure software update is a complex task. Companies want to outsource that complexity and concentrate on their unique value added application in the device and in the cloud. ■■



WHY A TRUSTED DEVICE EQUALS TRUSTED DATA

Security starts even before establishing the root of trust to secure devices and the data they generate, store and transmit from the chip right through to data hitting the cloud, writes Annie Turner.

We are heading towards a predicted one trillion connected devices by 2035, but security remains a big fear for many companies and consumers who are thinking about deploying IoT. It is such a big issue that some pundits think it could slow IoT's promised growth and associated economic benefits: in October 2018, research published by Bain & Company stated that securing IoT was the biggest concern among 45% of executives from enterprises it surveyed.

Importantly, the research identified securing devices as a key factor in securing the data they generate, store and transmit, and predicted that customers would be willing to pay 22% more for secure devices and buy 70% more of them. This would, according to Bain, grow the IoT cybersecurity market by US\$9 billion in 2018 to US\$11 billion in 2020. An article in The Economist about IoT security in September highlighted **Arm** and **Intel** as having moved to fortify devices by building security into their chips. ▶

HOW DEVICE MAKERS CAN REAP BIG REWARDS

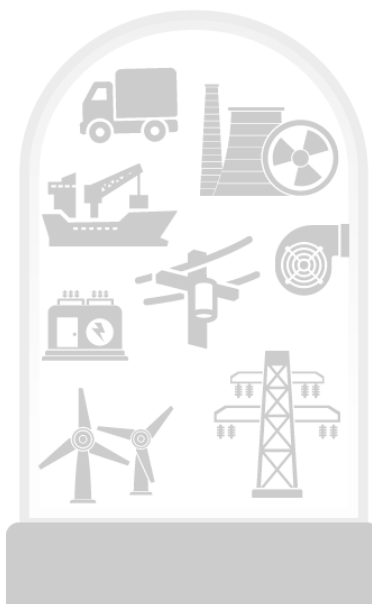
Manufacturers can gain market share by doing four things



Understand how customers use their devices
Stay current on usage patterns to help identify unmet needs



Certify that devices aren't vulnerable
Use cybersecurity best practices to deliver a hardened device

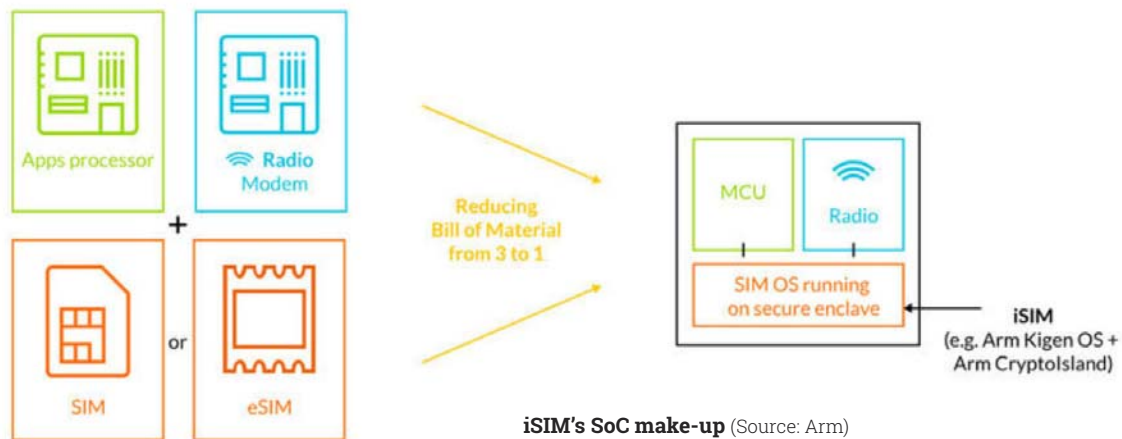


Build cybersecurity capabilities into more devices
When possible, partner with trusted vendors to provide additional solutions



Continuously test and update for new vulnerabilities
Use the warranty period to deliver updates that fix newly found issues

Source: Bain & Company IoT Security Infographic



IoT applications will run on cellular and non-cellular infrastructure for years to come, but Francis D'Souza, the vice president of strategy, analytics & IoT at **Gemalto**, points out, "When it comes to the data transmission between the device and the backend server, cellular transmission is inherently more secure than other means because of the inherent authentication and encryption present due to the subscriber identity module (SIM) and telco networks. And new, dedicated cellular IoT networks such as CAT-1, CAT-M and CAT-NB IoT are being rolled out by customers – they make adopting cellular a lot more cost-and-power efficient than previously, along with all the in-built security on the device-to-cloud path."

Clearly the evolution of SIM technology will play a critical role in helping to secure cellular IoT devices, primarily in the shape of the **GSMA's** embedded SIM (eSIM) standard and Arm's integrated SIM (iSIM). Yet as Vincent Korstanje, the vice president and general manager, Emerging Businesses at Arm, highlighted in August, a survey of 650 executives indicated there is considerable resistance to and a lack of knowledge about them.

The survey found that the three greatest obstacles to large commercial eSIM deployments were resistance from established stakeholders (69% of respondents), the perceived complexity of delivering eSIM deployment (40%) and concerns about being locked in (40%).

Further, although 90% of respondents knew about eSIM, 43% were unaware of iSIM technology. The respondents came from mobile operators, chipset and module makers, original equipment makers (OEMs), IoT service providers, enterprises, consultants and SIM vendors.

So what are eSIM and iSIM?

eSIM stands for embedded subscriber identification module and is a standard drawn up by the global mobile network operators' trade body, the GSMA. This universal approach will grow the Internet of Things by allowing

manufacturers to build a new range of products for global deployment based on this common eSIM architecture.

Moving away from providing a pluggable SIM slot and adding the eSIM into the device adds complexities in sourcing, manufacturing and requires knowhow which all act as a barrier to adoption. In addition, even an eSIM can consume precious space in a device and could be the make or break of being able to serve a size sensitive use case. An iSIM solves the space conundrum as it resides within the footprint of the System on Chip (SoC), which is already a necessary IoT device component. It also removes the technical integration angst from the device manufacturer at device assembly.

An iSIM runs within a security enclave, implemented as an integral element of a SoC. The security enclave introduces dedicated, protected processing and isolation for the execution of eSIM functionality whilst residing alongside other system on chip components including microprocessors and the cellular module. Arm's integrated SIM (iSIM) implementation offers full compliance with the GSMA's eSIM technology.

The advantages of this approach are greater security – in part by reducing the attack surface to one component – a smaller footprint and reduced power requirements for operating cellular IoT devices in remote locations and at an economically feasible cost.

Security first

The first part of securing a device is using a secure boot to activate it. D'Souza stressed that only a hardware-based root of trust should be used to provide an immutable source within the cryptographic system and it must be isolated from the wider operating environment. Secure boot ensures the code that runs on the hardware platforms is authentic and unmodified, from the first piece of code – the microloader – that boots to establish a root of trust, on which all the next interlinked measures build. ►

“ Identity is another piece of the security jigsaw. Each device needs a unique and secret identity, according to D’Souza, as it must always be clear which device is communicating ”



Francis D’Souza
Gemalto

He warns that if secure boot is not implemented properly, a hacker could inject malicious code and change what the device is meant to do, without the device owner even knowing, with potentially devastating consequences. This is what happened in October 2016 when a huge distributed denial of service (DDoS) attack disrupted about a third of all US and some European internet services.

Millions of IP surveillance cameras, printers, baby monitors and other apparently innocuous devices were infected with the Mirai virus by hackers who had correctly assumed that the devices’ default usernames and passwords were unlikely to have been changed when they went into use and used them to carry out an orchestrated attack on **Dyn**, the domain name server which maps browsers to web sites.

D’Souza adds, “The implementation is as important as the technology, if not more important because if you have [badly implemented] technology in place, you might be more confident than you should be and less vigilant.” No wonder the consulting firm EY’s recent study about the Smart Home found that 71% of the 2,500 consumers it surveyed were worried about hackers gaining access to smart gadgets.

On the other hand, done properly, the secure boot procedure with a protected root of trust ensures all the devices are linked and hackers cannot intervene. An industry certified security enclave, realised within the SoC, can offer such root of trust protection and is in line with Arm’s PSA.

Arm’s Platform Security Architecture (PSA) framework provides a reference against which IoT developers can realise product with security inherent. It has been formulated to provide an industrywide, standardised approach to building secure multi-vendor ecosystems of IoT hardware and software. It comprises a set of application programming interfaces (APIs), best practices, threat models and opensource reference firmware. The PSA methodologies are available to all vendors and developers to build products against.

Arm also believes that this root of trust can be co-located with the iSIM, within the security enclave, without compromise due a SIMs security architecture. An iSIM, running a SIM OS such as Arm Kigen eSIM OS, offers full industry standardised functionality and complaint, accredited and certified remote management. Arm is working within the industry standards community to realise the delivery of IoT device root of trust at point of manufacture.

iSIM also runs on Arm’s Kigen operating system software stack which provides a high-level of isolation and security, suitable for stringent certifications.

Lifecycle management

Devices’ identities (see below) are typically in the form of keys, which are used to derive various things, including certificates to enable the encryption of data from device to the cloud or to sign and verify data. The certificate is inextricably linked to the encryption algorithms themselves, and typically has a limited life span of three to four years.

This is deliberate as otherwise, given enough time, a hacker could listen in to transmissions and with sufficient compute power – the cost of which is falling all the time – eventually crack the encryption. D’Souza says that in “the normal world” this is not such a big issue, but in IoT, where devices could be in place for perhaps 15 years, the need for “hygiene and best practices” is acute and constant.

He explains, “You need to stay ahead of hackers – you always have to assume the worst. If I have one million smart devices out there and someone is waiting to carry out an attack from them all at the same time they could cause terrific damage. Updating the identities, that is the keys, on devices every month or two, reduces the risk and the hacker is back to zero.”

A unique identity

Identity is another piece of the security jigsaw. Each device needs a unique and secret identity, according to D’Souza, as it must always be clear which device is ▶





communicating. He recommends implementing a diversified identity, which he acknowledges is, “not rocket science”, but adds, “doing it well is critical: if, for example, you have a secret identity for a million connected devices, those IDs need to be stored securely on the devices to avoid being cloned, but also secure where the identities are generated from and stored, whether on a server or the cloud, or they could be spoofed.”

He refrained from revealing the company in question, but reported a recent conversation he had with an organisation that explained it did not need diversified identities as it used the same identity on all its devices. As D’Souza notes wryly, in such a situation, how would it be possible to know which is an original device and which is the clone?

Updating applications

During such a long operational lifetime, there are bound to be updates to applications, which again is a potential source of incursions. If upgrades are not properly managed, there could be an attack from the internet.

Again, design is foundational: D’Souza says the device must be designed so that it only accepts secure updates from a trusted server and the updates are signed and scheduled. There must be authentication between the server and device, via a public key infrastructure (PKI), that ensure the device won’t accept an update from anywhere or anyone else.

He stresses, “If you implement right, then you can update – security is a constantly moving target” as was so painfully shown by the the massive, so-called side-channel attacks, Spectre and Meltdown, in 2017.

Simon Segars, the chief executive of Arm, noted in the *Arm Security Manifesto 2018/19*, “What the researchers found [when they investigated Meltdown and Spectre] went to the heart of decades-old perceived wisdom about processor design. It under-lined how ‘secure’ is not a permanent state, only a judgement at a point in time that must be constantly revisited.”

Security is collaborative

As Yossi Naar, chief visionary officer and co-founder of **Cybereason**, which provides a cyber defence platform for endpoint prevention, detection and response and active monitoring, observed, “While cybercriminals can succeed even if they act independently of each other, our industry will only win if we act together.”

Segars concurs with this, adding in the same article, “In the case of these new side-channel attacks, an in-house team at Google found the threat, and our industry’s response – in particular Intel, **AMD** and Arm as lead partners – was immediate and carefully handled. Cost was never a factor, and companies across the sector collaborated at a depth and scale that I’d never seen before.”

Complexities of cost

D’Souza notes, “The cost of hacking keeps going down”. He says that a hack that would have cost US\$30 million to execute 15 years ago can now be carried out by a ‘script kiddie’ (a person with limited knowledge) who can buy the software for US\$300 from **GitHub** or any other such repository.

To counter to this, the only pragmatic approach is through a multi-layered approach and collaboration to make attacks on a system uneconomic. By increasing the cost, time and difficulty of attacks, it is likely that fewer will succeed. In addition to the other measures, this must include being able to detect and quickly identify threats in the field, so that threatened devices can be isolated, maintained and updated as necessary, to defend the integrity of the trusted firmware and the overall infrastructure and the applications that run on it.

However, these elements are typically handled by separate parties and it can be challenging to implement and coordinate their operation to guarantee continuity and trust. Again, collaboration, multi-layers and platform models come to the fore.

Cybereason’s Naar said in his contribution to the *Arm Security Manifesto 2018/19*, “As an industry, we need to support defenders in



Yossi Naar

Cybereason

taking a proactive approach to security. Instead of waiting for security tools to generate alerts (how security is traditionally done), we need to focus on threat hunting – looking for attackers already lurking in an environment.

“Now that we are working with Arm and its Pelion IoT Platform, we will have an ability to take an overview of any device in a connected network that is running the Arm Mbed OS,” he added. “This means remediation action can be taken if a threat is detected anywhere in a network. Detecting threats across a deployment is vital as hybrid networks made up of IoT devices and non-IoT devices become more common.” ■

SHOULD YOU MANAGE YOUR DEVICE DATA ON THE CLOUD OR ON YOUR PREMISES?

The consensus on the best way to manage IoT device data has flipped. Advocates for managing the information on computers in-house have lost their majority in a massive swing in consensus. The conventional wisdom about cloud management has changed from why to why not, writes Nick Booth.

The in-house party isn't so small that they could lose their deposit - but it's heading that way.

Hima Mukkamala, the senior vice president and general manager of IoT Cloud Services at **Arm**, has an explanation. The public cloud deploys faster and offers low entry costs, minimises the customer's need for a data centre infrastructure and changes the financing from the rigid formality of capital investment to a flexible operational cost.

On the other hand enterprises that run their own systems 'on-premise' have greater control and governance of their data,

says Mukkamala. "This supports faster decision-making, tighter security and a system that runs even where there's no internet coverage. So a water company that's governed by strict regulations on where its data can go and who can access it is better served by on-premises deployments."

In this niche of the Internet of Things (IoT) the cloud doesn't fit with every data manager's philosophy. In this niche localised control can be more of a priority. Machine to machine (M2M) communications run to a different rhythm because - as automatons - neither end user is constrained by the fatigue, capacity or speeds of input limitations that humans have. ►



Which means they have a voracious appetite for consumption - and therefore transport and storage - of data in either greater volumes or a fraction of the delay - possibly both.

Data protections and data management are much easier in the cloud, says **Druva's** chief technologist, W.Curtis Preston. Why? Because the likes of Amazon Web Services (AWS) and Microsoft with Azure have based their entire business on honing these specialist skills. "So there is no way you can do it better or cheaper than they can. There are no savings to be made trying to build your own infrastructure," says Preston.

You can't get better security than **AWS**, which has the most closely vetted centres in the world, according to Preston. "The cloud isn't the wild west any more so nobody needs to lay their own roads or build their own bank," says Preston.

There are political reasons why you should never run your data management systems on your own premises, Preston says. These are routed in human foibles rather than machine failings, so there is no technical fix.

Backup and recovery is a vital job, but is incredibly boring and unrewarding. It's a low status job that nobody wants and is invariably defaulted to the office junior. Which is a fatal mistake, given that data is the lifeblood of the company. Emergency transfusions should not depend on the operational skills of the hospital's work experience trainee.

"I've been doing this job 25 years and never seen anyone want to do the backup and recovery," says Preston. This means that on premise back up and recovery dangerously compromises performance, the likelihood of recovery and the degrees of security.

By contrast, software as a service (SaaS) for data protection is fine-tuned by almost perfect competitive market conditions and a skills base matured by decades of experience.

The only circumstance where data protection is not compromised by DIY savings is when the data amassed is static, unchanging and in such vast volumes that the economies of scale outweigh the saving from paying a service provider. Which is very rare, since service providers do everything more efficiently. This would happen if you have a single data centre with tens or hundreds of petabytes of uniform data.

On the whole, IoT is unlikely to generate data that is static. IoT deployments are dynamic in nature.

There are more likely to be circumstances in which thousands of devices are each giving off tiny records which are unlikely to be subject to rapid and constant examination. For example, devices that measure temperature and humidity in an environment that rarely changes.

There are two options for protecting your data in the cloud. You either buy software and run it on your own virtual machines or you get a software service provider to do it for you.

"Running your own software on your own property gives you problems you have to own," says Preston. The most expensive problem is that this forces you to expertly guess the future - which is near impossible in any aspect of computing, let alone something as volatile as the IoT. Nobody can correctly predict their future needs for bandwidth, storage and processing power. If you could predict the future, you wouldn't need all those measuring devices out there monitoring all the variables. Even backup and recovery are unpredictable.

If you buy a service to do all this, it will run on the SaaS provider's systems so they take responsibility. The SaaS provider can optimise for the cloud and coax the best possible performance with totally predictable costs.

One problem with the cloud is that the pricing plans are often tricky, says Martino Corbeli, chief product officer at integration platform maker **SpinR**. "It's a bit like going into a car showroom knowing what you want to get but being shifted into various pricing plans none of which quite fit."

Despite that one area of uncertainty, Corbeli says we are definitely going into a cloud first world because the savings made - by not having to worry about the peaks and troughs of variable data - will compensate.

There is no one size fits all solution. In circumstances where there is a wide diversity of needs, the versatility of a service provider becomes their most attractive quality, because it means they can tailor their supply to match your demand.

So your best bet is to look for providers who can manage all three options - in cloud, on-premise and as hybrid, concludes Arm's Mukkamala. ■■

GOOD DEVICE MANAGEMENT CAN UNDERPIN SUCCESSFUL DATA STRATEGIES

Potentially billions of IoT devices have to be securely deployed and managed from the chip right through to the data, whether that's on-premise, at the edge or in the cloud.

Antony Savvas explores device management throughout the device lifecycle.

When it comes to device management, the challenges are about far more than initial configuration and setup, they are about the ability to mitigate problems and flexibly change functionality during the life of the device, which could be deployed in the field for more than a decade in some IoT areas. While managing IoT devices and managing data from IoT devices are two related but separate issues, ultimately, good device management can underpin an organisation's successful data strategy.

That said, it is clear that the industry has a challenge on its hands. With the onset of digital transformation, the volume and diversity of connected devices in enterprises today has increased drastically. And while this might help companies introduce operational efficiencies into the workplace, it also leaves huge security gaps for those that are unaware of the pitfalls of poor device management.

Digital transformation

According to security vendor **Forescout**, it can be estimated that any business undergoing digital transformation has about 30-60% more devices on its network than the IT department actually knows about.

Chris Sherry, the regional vice president of EMEA North at Forescout, says: "Naturally, when asked to imagine devices in the workplace, most people immediately think of smartphones and laptops. But what about the printer that sits in the corner of the office, or the surveillance camera monitoring the car park? Not only that, but development in industrial IoT (IIoT) has meant that operational technology such as sensors, actuators, controllers and even light switches are all becoming IP-enabled too despite the fact they were never intended to be. As a result, IT teams are scrambling on how to account for them and manage them."

Sherry says a major factor to overcome is that different lines of businesses don't see eye-to-eye on what the management strategy should look like. "To gain full control and visibility of all devices on a network, enterprises need to use tools that consolidate them into a single, unified device visibility and control platform. It is all about IT asset management (ITAM) with better streamlined visibility and automation," he says.

Remote monitoring

Manfred Kube, the head of communications, analytics and IoT Solutions at **Thales**, says: "For most IoT use cases, it is virtually impossible to send regular physical maintenance workers to each and any device as this would be time consuming and kill your total cost of ownership (TCO)."

Kube adds that the most efficient approach is to use analytics tools that monitor IoT devices remotely and address challenges in real-time. Companies must deploy integrated and connected hardware solutions, plus strong encryption schemes, to ensure efficient management and tight security to enable devices to be patched with the latest software, firmware, applications and security, that will enable them to evolve to support new use-cases in the years ahead.

Cloud providers

To help deliver what is required, a number of IoT providers are building ecosystems to enable comprehensive solutions that address all segments of the market. This includes the involvement of big cloud service providers **Google, Microsoft** and

Amazon that have tailored solutions. Each of these three can help partners and customers to securely provision, authenticate, configure, control, monitor and maintain all of their IoT devices.

The importance of addressing the evolving edge networking environment is also coming into play. IoT devices will increasingly be located closer to customers at the edge to help reduce latency, for applications such as 5G, artificial intelligence and driverless cars.

From a device management perspective, the biggest problem is going to be updates. For most large organisations, it's hard enough to keep every desktop and laptop device up to date, let alone the addition of hundreds of new devices at the edge of a network.

The evolving ecosystems to support IoT device lifecycle management can be illustrated by the approach **Arm** has taken. Its Pelion Device Management aims to provide simple, secure and flexible IoT management capabilities for a range of device profiles. Multiple deployment configurations are available to suit the customer's needs, including cloud and edge options, an on-premise solution with cloud-like capabilities or a hybrid of the two.

About a year ago, Arm acquired **Treasure Data** and brought together its data management technology with Arm Mbed Cloud solution, in addition to connectivity management technology resulting from its acquisition of **Stream Technologies** to launch the Pelion IoT Platform.

The Pelion IoT Platform consists of three major components covering device management for provisioning, identity and access management and updates; connectivity management to support wireless connectivity standards for any device and the enablement of eSIM secure identification; and data management for the analysis of trusted data from individual devices and enterprise-wide and third party big data deployments.

Standards

When considering any solutions though, it is also important to consider standards and best practice, which is something that non-profit organisation **GlobalPlatform** is supporting.

Driven by around 90 member companies, the organisation develops international standards for enabling digital services and devices to be trusted and securely managed throughout their lifecycle, when deployed in the payments, telecoms, transportation, automotive, smart cities, smart home, utilities, healthcare and government sectors.

Gil Bernabeu, the technical director at GlobalPlatform, says: "Many connected devices – such as connected cars and machinery – could have lifecycles spanning decades. Effective device lifecycle management is therefore essential for the security and functionality of all IoT devices and their networks. Devices that cannot update their software, permissions, firmware and security in-field should not be brought to market in the first place."

A clearly defined process to manage device end-of-life is also fundamental, says Bernabeu. Whatever the device and whatever the environment it is functioning in, it is clear that its deployment and on-going management have to address key fundamentals to deliver the full benefits. ■■

DEVICE DATA DEMANDS MANAGEMENT STRATEGY AND AUTOMATION AT HYPERSCALE

As IoT matures and the numbers of connected devices start to soar from a relatively low level into the billions, the greater challenge for organisations employing IoT could be more in managing the device data than in managing the devices themselves. If there are billions of devices there will be trillions of data points transmitted on a daily basis. George Malim explores how all of this will be managed from the chip on the device through to the cloud, edge or on-premise data processing capability.

The sheer scale of data involved means that organisations cannot hope to address the challenges of managing IoT device data with casual approaches that involve applying technologies retrospectively. Technical frameworks, policies for ingestion, transforming and prioritising the data along with methods to assure compliance to regulations all need to be thought of, planned for and designed, ideally in advance of deployment. The sheer volume of data is a huge obstacle because only parts of IoT-originated data are valuable. This means that organisations need the capability to automatically sift and prioritise it to avoid the expense of processing, analysing and acting upon everything.

"In order to manage IoT data effectively, there has to be an overarching business strategy, matched up with supporting technology," explains Peter Ruffley, the chairman of **Zizo**, a provider of edge analytics. "IoT data is in reality no different to any other type of data that we are creating with two big exceptions: one, there is a huge volume of it; and two, most of it is completely worthless."

The issue of apparently worthless data is significant here because there's often a feeling that all data contains at least some form of hidden value. Maybe it does, maybe it doesn't but storing it and analysing certainly involves cost. "One of the key issues here is that organisations expect to have to keep all of this data, due to the fact that there is a belief that there may be some value within it in the future," confirms Ruffley. "This is most likely not the case and is why there needs to be a clear business strategy in place to best manage any IoT project." ►

“
Some data is processed
at the edge in relatively
intelligent devices,
thereby minimising what
is communicated for
central processing, while
other data is simply
shipped wholesale to the
cloud for analysis
”

“This won't be a one size fits all approach, but rather a combination of solutions in various locations – edge, cloud and on premise – which throws up its own challenges from a data management perspective,” he adds. “Data ownership is also a key challenge; understanding who owns what data, and what can be done with it will become a major part of the IoT data management lifecycle.”

Joel Chimoindes, the vice president of **Maverick AV Solutions** Europe, agrees that a first step is to gain understanding of where the value lies in the data you have. “In order to manage data effectively you have to understand first what data you need and what data is relevant for your business - your insights, the objective, the business outcome,” he explains. “Having decided what data you require, you should think about how to model and store that data.”

As a specialist in the audiovisual industry, Chimoindes gives the example of the challenges associated with data in digital signage. “The place where we come in is about how to collect and then communicate that data,” he says. “The main challenge of this is the sheer scale of digital signage networks and then the opportunity that AV endpoints offer for businesses. The proliferation of them means you have to be very clear what you want to achieve through an IoT project and how that will benefit your business.”

The disparity of devices adds a further layer of variation that device data strategies must address. “You have the [data] generating device to consider,” points out Fredrik Forslund, the vice president of enterprise and cloud erasure solutions at **blancco**. “You have to work closely with manufacturers and understand what storage capabilities and security you have on the device. There will be quite smart ones like smart speakers and TVs and very stupid ones that are less intelligent and can't do much more than broadcast some data via a GSM chip to the cloud.”

With all this data comes responsibility and Forslund is keen to emphasise that even with the hyperscale volumes of data generation, organisations still are bound by data regulation. “IoT generates a lot of new data and that generally goes straight into the cloud – either public or private,” he says. “Even so, someone has to be responsible for the data and then manage the lifecycle of the data from generation to ultimate erasure.”

Being responsible with IoT data is both a weighty burden and a potential key point of failure for IoT initiatives. “The rapid growth of IoT caused by expanding connections of unsecured end points, when combined with progressively worsening network attacks and system intrusions, has dramatically raised the risk exposure for unsecured networks to levels beyond most companies' ability to calculate,” says Phil Celestini, the senior vice president and chief security and risk officer at **Syniverse**. “This emerging reality in turn calls into question previous risk acceptance decisions for connecting business systems to the public internet.” ▶



Phil Celestini
Syniverse

So what are organisations doing to enable them to manage device data securely and responsibly? In essence, they're turning to technology vendors to supply them with the data processing platforms they need to first handle scale and second uncover the value in the data. These vary widely depending on the data being collected and the format in which it is communicated. Some data is processed at the edge in relatively intelligent devices, thereby minimising what is communicated for central processing, while other data is simply shipped wholesale to the cloud for analysis.

"A huge variety of platforms are being used and developed to meet these needs," confirms Ruffley. "These range from big cloud platforms like **Microsoft Azure**, down to [offerings from] specialist hardware and software vendors. Technologies such as time series databases which enable the analysis of data over time, through to NOSQL or NewSQL databases, which allow for high volumes of data alongside standard query technologies, for near real-time query, or **Apache Spark** for real-time data analysis and streaming, are being deployed. The main focus here for organisations is picking the right tool for the job; with a key understanding of what the costs will be at scale."

For Chimoides, effective data management is a complex equation involving six key areas – data gathering, transportation, storage, security, analysis and action – that must be addressed. "First is gathering the data, does the customer already have the means to measure particular data, or do you need new sensors need to be added?" he says. "Next is transportation. Moving large amounts of data can be costly and is also crucial to the success of IoT. Is a wired or wireless set-up ideal, will sensors feed straight to the cloud, or will you run on a hybrid of edge computing mixed with the cloud? This leads into the question of where will your data be stored."



Joel Chimoides
Maverick AV Solutions

"Once you have established what data is to be gathered and how, you must ensure all this information is secure," he adds. "There should be a security layer on the level of every sensor, the gateway or edge level and the cloud."

"Analysis comes next and is when you can start to begin to search for solutions from the data you have collected using edge or cloud solutions to derive patterns that can then be solved," he continues. "Finally, action. From the data gathered what rules, alarms or actions can be set up to improve the customer's workplace?"

This list is not exhaustive but it does help to lay out the sheer scale of the problem and the number of disciplines involved in device data management. This will require specialist expertise and inevitably human decision-making, even though automation is a prerequisite because of the sheer scale of data involved and the speed of data processing required.

"Due to the complex nature of any IoT deployment, there will be a requirement for specialist skills and expertise," says Ruffley. "But, it is important to note that we must still hang onto first principles, which are how do we get the right data to the right people at the right time? This requires input from all areas of the business, including data science. As always, business engagement will make or break any analytical project."

Chimoides also acknowledges that human specialists are needed. "In the planning, installation and execution of an end-to-end solution, experts are still required at multiple levels," he says. "The key figure is the solution architect to oversee the operation and then a human developer is still required to craft algorithms and patterns. The depth of understanding of the business and then what is possible in IoT will be the key to truly transformative solutions." ►



Fredrik Forslund
blancco

Forslund agrees. "Everyone is looking for the ability to automate and integrate into the common process but sometimes that isn't possible," he says.

Ruffley sees technologies coming to the aid of business engagement, allowing greater intelligence to be automated. "Machine learning is going to be very important to battle the raft of data that is flowing into the IoT architecture, however, we have to create solutions that meet the first principles I mentioned earlier," he adds. "This requires a new look at the data flow – from device to processing, and edge computing has a big part to play in sending the right data to tools and technologies to be accessed by individuals who can make a difference."

New market requirements often result in new approaches from solution vendors and the area of IoT device data management is no exception. Chimoindes cites the aggregation of solutions from multiple vendors as a means to simplify the landscape for organisations. "Multiple vendors and products are needed in a single solution, so trying to make this packaged and repeatable is the key to success," he says. "We are seeing manufacturers for the first time working together to create common protocols and solutions which can be scaled globally."

Ruffley sees increased deployment of edge computing capability as another transformative technological lever. "The emergence of edge computing with connected micro data centres, such as **Vapor IO**, is taking the heat from the cloud data centres," he says. "Also, with the creation of Microsoft Azure Stack and **AWS** Outposts, the bigger players are seeing a need to push processing further out into the wild. Finally, we are seeing some interesting hardware developments with players like **Intel** and **Lenovo** with their SE350 server simplifying data management at the edge."



Peter Ruffley
Zizo

In spite of vendor efforts to simplify device data management, the complexity of integrating data from multiple different devices and then analysing it to create valuable insights can't be underestimated.

"The challenge is the same as integrating data from multiple different data sources to meet those goals: it's very difficult without the right business strategy and the right technology in place," says Ruffley. "That being said, the problem is not insurmountable; the trick is working with the device suppliers to understand data formats, and working out what data is actually needed to deliver your insights that meet the defined strategy. Many organisations will have some form of data management strategy in place, but they will have to look at the scale of what they need, and what they don't need to meet these objectives."

For Chimoindes, just because something is complicated doesn't mean it's difficult. "Integration is complex, however there is no reason it has to be a challenge," he says. "As long as you are crystal clear on what you are trying to achieve, and when you specify the solution this is part of the application from the start then technology is no longer a gatekeeper to smart solutions such as IoT."

Data management doesn't end until the life of the data is concluded with its secure erasure from the system and all the devices. "The area has been neglected because there's a business rationale to focus on the top line of generating revenues and increasing value by having data and the ability to analyse it," says Forslund. "However, the need to manage data from first collection right through to its erasure cannot be ignored. If you delay thinking about this to the future you'll increase the impact of the challenges." ■■

“
The emergence of edge computing with connected micro data centres, such as Vapor IO, is taking the heat from the cloud data centres
”

arm PELION

The Device to Data IoT Platform for Intelligent Enterprises



Learn how Pelion
can simplify your
IoT transformation
at [Arm.com/pelion](https://arm.com/pelion)

- + Flexibility in design, deployment and connectivity
- + Support for any device, any network, any cloud, and any data-type
- + Efficiency of IoT adoption
- + Infuse chip-to-cloud security in your IoT deployments