CSO Insights
FROM IDG

Issue: **February 2018**

THE COMPLETE GUIDE TO: INTERNET OF THINGS

Credit: iStock

Produced by IDG

Credit: iStock

Connected world

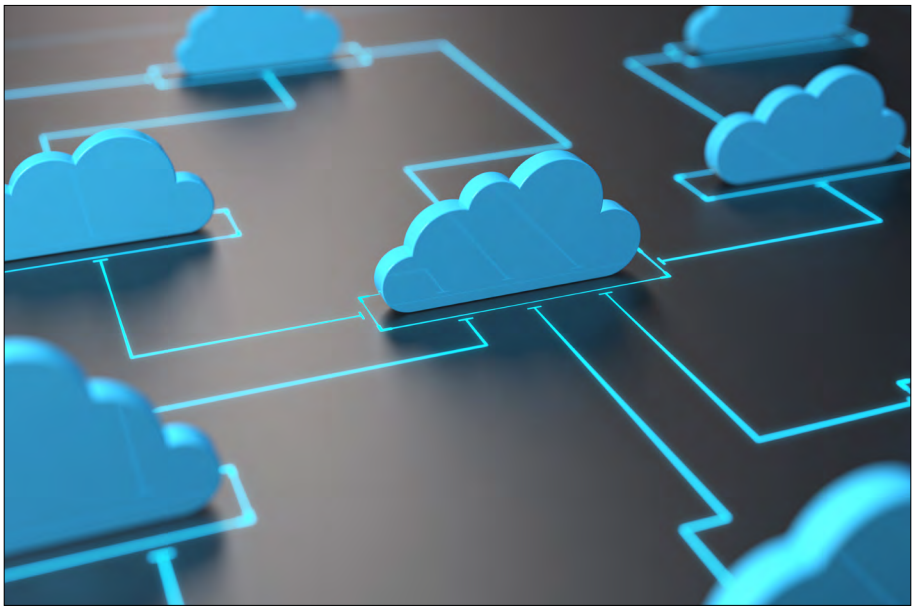
The Internet of Things (IoT) has been a hot topic in the enterprise technology world for some time, but we are only now starting to see true end-to-end IoT solutions and case studies in the wild. By connecting up fleets of Internet-enabled devices and the huge volumes of data these generate, businesses can start to get a better handle on their assets, save on maintenance costs and leverage critical efficiencies.

The use of IoT at enterprise scale isn't limited to industrial IoT (or the industrial Internet, as it is also known), but consumer-facing organizations such as British Gas, insurers including Aviva and the healthcare

industry are also starting to leverage IoT technology to the benefit of their customers.

Here we demystify some of the key terms and technology involved with IoT (edge computing, anyone?), run through the best tools and platforms technology vendors have built for managing devices and data, offer some security advice, and run through real-life case studies of organizations putting IoT to good use. **Scott Carey**

Contents



Credit: iStock

Best cloud IoT platforms

We run through the major cloud IoT platforms to manage devices, store data and mine insights from connected assets

As businesses look to adopt the Internet of Things (IoT) by connecting Internet-enabled devices to assets and relay that information back to key decision makers, the need for a platform to store, manage and analyse all of this data is increasingly important. The good news is there are lots of options in the market, with all of the big players in public cloud (AWS, Azure, Google Cloud Platform and IBM) providing IoT platforms, as well as smaller pure-play options for more industrial IoT (IIoT) uses. The bad news

is this means the IoT platform market can be a bit of a jungle, with all of the big players promising the easiest, smartest platform available.

Here, we run through the best IoT platforms for your business, to help you get the most out of those connected assets and the data being driven by them to creating operating efficiencies and maybe even whole new business models.

1. AWS IoT Platform

URL: fave.co/2mFEfqw
Cost: $5 per million messages

The AWS IoT Platform provides a device SDK, secure device gateway, registry for recognizing devices, device shadows (a virtual version) and a rules engine to evaluate inbound messages.

Simply put, the platform provides a place to connect and manage sensors – on cars, turbines, sensor grids and light bulbs for example – by using AWS' public cloud to store, process and analyse the data transmitted by these devices.

AWS has also struck up partnerships with the likes of Broadcom, Intel, Qualcomm and Texas Instruments to create hardware component 'IoT Starter Kits' that are compatible with its services.

The vendor also released AWS Greengrass in November 2016. This software allows customers to run local compute, messaging and data caching at the edge, so on the connected devices themselves. Using AWS Lambda functions, Greengrass keeps device data in sync, and lets them communicate with other devices securely, even when not connected to the Internet.

2. Microsoft Azure IoT

URL: fave.co/2mGCvNF

Cost: Free for up to 8,000 messages per month, £37.27 for up to 400,000 per month, £372.66 per month for up to 6,000,000 messages and £3,726.55 for up to 300,000,000

Running alongside Microsoft Azure cloud services, the Azure IoT Hub offers a rules engine, identity registry, information monitoring and device shadowing.

The IoT platform incorporates existing products such as IoT Hub, Stream Analytics, notifications hubs, Power BI and some pre-packed machine learning to process and analyse large quantities of device data in near real-time.

For example, Rolls-Royce is using Azure Stream Analytics and Power BI to link up sensor data from its airline engines with more contextual information like air traffic control, route data, weather and fuel usage to get a fuller picture of the health of its aircraft engines.

Using Microsoft's Azure IoT Suite to collect data and Cortana Intelligence Suite to derive insights, Rolls-Royce can go beyond predictive maintenance and into metrics that it can pass onto operations teams at airlines as a value-added service.

3. Google Cloud IoT

URL: fave.co/2Dqh2Dq

Cost: Between $0.0045 to $0.00045 per MB depending on the volume of data exchanged by IoT devices with the service after the 250MB free tier

Google looks to set its IoT platform, which sits on top of the Google Cloud Platform, apart from rivals through

its focus on 'intelligence'. This means you can connect, manage and ingest IoT device data to the Google platform before running advanced analytics, like ad-hoc queries using Google BigQuery, applying machine learning with Cloud Machine Learning Engine, visualize data in Google Data Studio or even trigger automatic changes to devices based on real-time events using Cloud Functions workflows.

So, the Google stack looks roughly like this: device data is captured by the Cloud IoT Core, this is published to Cloud Pub/Sub ready for downstream analytics. Google also supports out-of-the-box integration with IoT hardware makers such as Intel and Microchip.

4. IBM Watson

URL: fave.co/2mEwZve

Cost: You can trial IBM Watson IoT for free. The platform is pay-as-you-go after that, charged per MB of data processed

IBM Watson IoT is a platform for customers to connect all of their devices and IoT device data into a repository, where the cognitive capabilities of Watson can be leveraged to gain insight into an IoT network to improve operations and even launch new business models.

IBM Watson users receive device management, real-time data exchange, secure communications and data storage as part of the IoT platform.

For example, Finnish escalator and elevator manufacturer KONE has been using IBM Watson IoT alongside Salesforce software to manage its connected assets, which carry as many as one billion people every day. By combining intelligent analysis from IBM

Watson IoT with Salesforce's Service Cloud Lightning and Field Service Lightning tools, the company will be able to respond to emergencies as they happen.

5. SAP Leonardo

URL: fave.co/2Doioyl

Cost: Naturally pricing for a product like Leonardo will be bespoke, as it comprises various cloud software components, but SAP will also be pre-packaging options around certain use cases

German software giant SAP relaunched its Leonardo platform in May 2017 as a 'digital innovation system' after it was initially launched as an IoT platform.

The aim is to allow customers to take advantage of a broader range of emerging technologies than just IoT, such as artificial intelligence, machine learning, advanced analytics and blockchain.

That doesn't mean Leonardo can't be used for IoT though, and it already is. Heavy machinery manufacturer Caterpillar is eyeing Leonardo for vehicle insights, Trenitalia is using it for predictive maintenance on its trains, and UK SAP customer Northern Gas Networks is also looking towards Leonardo in the future for a whole host of IoT use cases across its massive gas distribution network.

Mala Anand, executive vice president of analytics at SAP, said at the Sapphire event in Orlando, Florida this year: "The intent is to bring together everything from machine learning, big data, analytics and IoT, all integrated and stitched together on our cloud platform. At the end of the day, we want to deliver outcomes and to deliver those outcomes to transition a business

outcome or business model. That cannot be delivered with just one technology."

6. Dell IoT

URL: fave.co/2mElwvr
Cost: Too early to tell, but pricing will almost certainly be bespoke

Dell Technologies announced a new IoT-specific division at an event in New York in October 2017, with the aim of combining its strengths in hardware with its Dell Gateway devices, the VMWare Pulse IoT Centre, and a range of consulting services, to help customers launch IoT projects quickly.

So the ideal, integrated stack for the vendor looks roughly like this: connected devices are managed near the edge using Dell Gateways, the VMWare Pulse IoT Centre is your window into monitoring and managing these devices, and Pivotal can provide a platform to build bespoke applications. Everything should be instrumented by Dell Technologies and connect back to the cloud environment of your choice, interact with any partner technology and then Dell also provides support.

This means that committing to the Dell Technologies stack becomes the primary consideration when signing up with the vendor.

7. Hitachi Lumada

URL: fave.co/2mE3h9w
Cost: Available on request

Japanese IT vendor Hitachi's IoT platform is called Lumada, and now sits under the Vantara big data

division at the company. Hitachi calls Lumada 'a portable architecture' which can be run both on-premises and in the cloud in order to support industrial IoT deployments. Naturally, Hitachi also speaks up its enterprise level AI and machine learning technologies, as a way for customers to solve problems before they occur.

8. Salesforce IoT Cloud

URL: fave.co/2mGtDaT
Cost: Available on request

Announced at Dreamforce in 2015, Salesforce's IoT Cloud runs on AWS infrastructure and provides customers with a platform to store and process device data. The platform is powered by Salesforce's proprietary real-time event processing engine Thunder, which is useful when customers are looking for real-time insight into how their connected assets are performing.

The benefit of IoT Cloud is the usual easy-to-use Salesforce user experience, meaning non-technical users can start to derive insights from IoT projects. Salesforce also added the MyIoT feature in 2017, which is a declarative interface for building apps on top of IoT data to create rules-based automation, for example.

9. Oracle IoT cloud platform

URL: fave.co/2mDxoOz
Cost: either $3.37 (£2.55) per hour on universal credits, or $2,500 (£1,900) per unit on non-metred services

Oracle's IoT cloud platform provides an end-to-end solution, from device virtualization and high speed messaging, to endpoint management and analytics for

real-time insights, all sitting on the Oracle PaaS cloud infrastructure. Oracle also offers pre-packaged IoT applications for use cases like asset or fleet monitoring.

10. General Electric Predix

URL: fave.co/2DpIscw

Cost: Available on request

Aiming to help organizations in industries such as aviation, healthcare, energy and transportation, Predix was launched by General Electric (GE) in February 2016 as a platform-as-a-service (PaaS) which supports the development of apps that can use real-time operational data to provide insight for better and faster decision-making around connected assets.

It has since been expanded to include a catalogue of GE and partner app templates to be used off-the-shelf with your IoT data, as well as a low-code Studio to help less technical users build industrial IoT applications.

The Predix platform can be used as a dashboard for managing IoT devices, customers can create digital twins (a virtual model) of assets to predict and optimize performance and leverage advanced analytics libraries to run machine learning on device data.

For example, Schindler uses the Predix platform to run predictive maintenance on its lifts and escalators to cut downtime of assets.

Predix can be run on any of the major public cloud infrastructure providers. Back in 2014 GE partnered with Verizon, Cisco and Intel to create 'Predix-ready' devices, and has more recently partnered with Apple to bring Predix apps to iOS devices to be used in the field.

11. Cisco IoT

URL: fave.co/2Dr8EDx
Cost: Available on request

Cisco provides IoT solutions and advisory services to help customers leverage IoT. The vendor's strengths lie in hardware, where it manufactures gateways and edge devices, but increasingly can provide management and monitoring through the Cisco Jasper Control Center, a Dev Centre for launching IoT applications, and security through IoT Threat Defence.

Originally aimed at mobile networks looking for greater visibility across their estate, Cisco has since worked with organizations like the Australia-based National Farmers' Federation to invest in IoT solutions within agriculture. **Scott Carey**

Credit: iStock

How to secure the IoT in your organization

Best practice tips and advice for Internet of Things security

All of the major technology vendors are making a play in the Internet of Things space and there are few organizations that won't benefit from collecting and analysing the vast array of new data that will be made available.

But the recent Mirai botnet is just one example of the tremendous vulnerabilities that exist with unsecured access points. What are the main security considerations and best practices, then, for businesses seeking to

leverage the potential of IoT? Read on for some advice on securing the IoT from the cybersecurity industry.

1. Read the literature

"Comprehensive security guidelines and industrial standards for IoT manufacturers would help," says Alex Mathews, lead security evangelist for Positive Technologies. There has been progress on this, and Mathews points to the Industrial Internet Security Framework published in 2016 – a collaborative project between players including Intel, AT&T, Hitachi, Fujitsu, Kaspersky, and many more – as a solid start.

There are other papers out there on the matter, including a 2016 White Paper from the US' Department for Homeland Security called Strategic Principles for Securing the Internet of Things. It warns: "Many of the vulnerabilities in IoT could be mitigated through recognized security best practices, but too many products today do not incorporate even basic security measures." Go to tinyurl.com/jL6qota for a more comprehensive rundown on advice from the US government.

2. Think long-term when choosing a supplier

Although budget constraints could make it tempting to opt for a newer business that promises the world or less well-known player at cheaper cost, keeping your network of devices updated is critical to security – so if your supplier suddenly isn't around anymore your organization becomes exposed.

"Make sure it's a well-known and reliable supplier that's likely to be around for the long-term," urges R&D director at Rocket Software, George Smyth. "IoT devices

need to be updated regularly when a new security flaw is discovered. If you bought from a company that has gone bust, you'll end up with a device that's basically useless. You need to buy from a manufacturer that will be around for years to come, so they can provide patches and fixes to any bugs that may arise."

3. Don't be part of the problem

In the wake of the Mirai botnet attack, Michael Marriott, research analyst at Digital Shadows, had this to say: "Don't be part of the problem. Secure your own devices and don't use default or generic passwords – and consider disabling all remote access to devices and perform administrative tasks internally. Instead of via Telnet, FTP and HTTP, use SSH, SFTP and HTTPS.asdf.

"To address DNS reflection, disable recursion on authoritative name servers and limit recursion to authorized clients," he argues. "To address NTP reflection, update ntpd to the latest version and disable the monitor function for legacy ntpd versions."

Go to tinyurl.com/y8bu29mL for Digital Shadows' Mirai and the Future White Paper.

4. Separate IoT from your business network

It goes without saying that the Internet is integral to the Internet of Things – but it's easy to lose track of exactly what that means. The IoT search engine Shodan (shodan.io) allows anyone in the world to browse thousands of Internet-connected devices.

Each and every connected device needs to be considered a potential access point for malicious actors.

"Businesses should place all IoT on its own VLAN, and that VLAN should not have routable access to the

internal enterprise business network," explains research lead at Rapid7, Deral Heiland. "The VLAN should also not be directly accessible from the Internet, and egress firewall filters on that VLAN should be configured to only allow IoT devices to connect to specific cloud IP addresses, as needed for cloud API communication."

"This method will reduce the risk and impact to an organization by reducing the exposure footprint. If there is a compromise, it should help isolate it outside the business network environment."

Verizon's *Data Breach Digest* (tinyurl.com/ha7dcxs) recommends that IoT systems should be air-gapped from critical networks wherever possible.

5. Protect and encrypt your passwords

Last year's MongoDB database ransomware was largely thought to have occurred in test environments – but not always test environments – where default or weak passwords were used. So it should go without saying that these should be changed. Again, basic security practice should be applied to the IoT network.

"Only large, complex passwords should be used," argues Rapid7's Deral Heiland. "This password should not contain any dictionary word or any part of the organization's name. It's also important these passwords be unique across the IoT technology, because this will help avoid the compromise of all devices within an organization if one device is compromised.

"And if the IoT technology utilizes its own wireless access point, it is critical that it be configured with the highest level of security possible – often this is WPA2 with AES256. The WPA2 Pre Shared Key should also be changed from default and a complex PSK should be

utilized, this shouldn't contain any dictionary words or any part of the organization's name."

6. Pay attention to the full network

Businesses taking advantage of IoT are increasing the range of the scale of their full infrastructure and by doing so create more potentially weak points in the chain.

"Organizations must look at the full IoT infrastructure from end-to-end and secure all points," says Winston Bond, EMEA technical director for Arxan. "A typical IoT framework consists of edge devices like sensors, adaptors and beacons, as well as a gateway to communicate with these devices, and a back-end server in the cloud or on-premises."

"Companies need to take each section separately and start addressing security issues for each," he adds. "From protecting the endpoints to hardening the binary code on the apps."

7. Don't count on the manufacturers

As with many nascent technologies, manufacturers don't necessarily consider the full security risks when they rush to build and release their products.

That's no exception for the Internet of Things, and although some will be more secure than others, it's best not to trust the manufacturers to have baked in security from the beginning.

"IoT devices are hard to protect and most were not made with any consideration to security," explains Peter Nguyen, Director of Technical Services at LightCyber. "They are built for easy connectivity to share information or receive instructions. Many lack robust access control or the ability to use secure, changeable passwords –

it's unlikely that effective endpoint protection software can run on such devices."

Rob Miller, head of operational technology at MWR InfoSecurity, believes that Manufacturers need to wake up to the fact it will also benefit them to design products with the latest attacks in mind, plus remote updating by default.

"There are no golden badges to look for when assessing a product's security features, so instead many consumers and businesses choose to buy from manufacturers that can demonstrate their interest in security," Miller says. "This might be in a warranty that includes security updates, or activity in the security community such as having a bug bounty programme." **Tamlin Magee**

Credit: iStock

What is edge computing?

Why edge computing signals a move from what is traditionally understood to be the cloud

Another shift in the technology landscape appears to be underway which has the potential to alter the way data is created and processed.

Edge computing is, in essence, tied to the evolution of the Internet of Things (IoT). As various industries push to connect previously dumb objects to the Internet, the way in which these objects talk to one another will change. For some uses, low latency is really crucial – think of a connected car needing to decided to avoid an object in the road – and so computing will need to take

place at the outer reaches, or the 'edge' of the network, nearer the objects themselves.

An edge device could be anything that provides an entry point to a network, for example, routers, WANs and switches. They will act as miniature data centres, able to communicate with one another – to form a 'fog' – and typically will be used for communicating urgent data.

For example, think of applications in automotive, manufacturing, fleet management, emergency and disaster response, where it is simply not prudent to transmit data back to a central data centre.

This will enable 'fog computing', a relatively recent term used to describe decentralised computing happening at the level of the object which requires data processing, rather than pinging complex requests to data centres that can be hundreds of miles or more away.

In November 2015, a coalition of vendors and academics active in the Internet of things field joined forces to create the OpenFog Consortium. The founding members are all heavyweights in tech: Cisco, ARM, Dell, Intel, Microsoft, and Princeton University.

The group's stated aim is to "accelerate the development of fog technologies through the development of an open architecture, core technologies including the capabilities of distributed computing, network, and storage as well as the leadership needed to realize the full potential of IoT."

Analyst group 451 Research estimates that the market for fog computing will overtake $18 billion by the year 2022, driven by utilities, transport, healthcare and industrial markets in particular. A working group created by the IEEE Standards Association is currently working

with OpenFog to hash out standards related to advanced IoT, 5G, AI and more relevant to fog computing.

General Electric, which is heavily invested in predictive maintenance and industrial applications for the Internet, says that edge is taking form now for a number of reasons, including, but not limited to: the lowering cost of compute, cheaper sensors, more power in small footprint devices like gateways and sensor hubs, the enormous swell of big data, and improvements to modern machine learning and analytics.

Imagine a single vehicle in an autonomous fleet, estimated by Intel to generate 40 terabytes of data for every eight hours on the road.

GE says sending all that data to a far-away cloud would be “unsafe, unnecessary and impractical” – this is because it is data that holds most of its value in the short term, and it requires extremely low latency for quick decision-making. The difference could literally be life and death. **Tamlin Magee**

Credit: iStock

Aviva embracing IoT to keep customers engaged

One of UK's biggest insurers is looking to bundle IoT sensors into its home insurance policies to foster customer loyalty

Aviva is increasingly turning to the Internet of Things (IoT) to set its home insurance offering apart from the competition. Through a range of partnerships with UK-based IoT start-ups, the insurer is looking to keep home insurance customers engaged year-round, and hopefully cut down on claims in the process.

Aviva breaks home insurance down into the three main issues its customers are most concerned by: safety, security, and leak. “Where that plays in is the new generation of cameras, sensors, smoke detectors and leak detectors, which give us this new capability,” says Nick Ayrdon, head of prevention and services at Aviva.

To harness these new capabilities, Aviva has taken the strategy of partnering with the best IoT start-ups in the UK rather than developing the technology itself. It has partnerships with home security camera company Canary, it holds a stake in Cocoon and is working with leak detection sensor LeakBot, developed by HomeServe Labs.

While leaks might not necessarily keep homeowners up at night, they certainly do insurers. Escape of water claims are the single biggest cost for home insurers, making up a quarter of all home claims paid out.

Aviva has been working with the LeakBot for over two years, allowing it to test the device in the field and gauge customer response. “The drivers for us aren’t just claims, it is about helping our customers keep their lives on track,” explains Ayrdon.

In terms of home security, Aviva gave away 500 Canary smart home cameras in October 2015 to new home insurance customers. Ayrdon says this exercise allowed the insurer to “harness all of the insights from that experience” but that it has not yet “integrated it into our product”.

Similarly, Cocoon is a UK-based smart home company which manufactures what it calls a “complete security system in a single device” and although Aviva hasn’t piloted the product with customers yet it has invested in the start-up through its ventures arm.

Customer engagement

The insurance industry is becoming increasingly obsessed with the idea of customer engagement, bringing it in line with important everyday services like your bank account through digital channels. “Most of the year customers aren’t using their insurance and aren’t making claims very often,” reveals Ayrdon. “So keeping us relevant is a big thing.”

The eventual aim for Aviva is to take all of these partnerships across those three tenets of home insurance – safety, security and leak – and to bundle it together for customers, ideally with everything managed via the MyAviva mobile app. So in practice a new home insurance customer wouldn’t just get a policy document but could buy a premium policy which sees them receive a smart home security camera and a LeakBot all at once.

“It makes sense to offer customers things that help them avoid bad things happening and whether they have adopted those themselves, or if we can offer it as a pack, that is something we are looking at,” adds Ayrdon.

HomeServe Labs

UK firm HomeServe has pivoted into IoT by spinning out a Labs division and developing the LeakBot, its leak-detecting sensor for homeowners, when it saw that existing leak sensors weren’t fit for purpose. The company’s core business has traditionally been home call-outs for home insurance emergencies and repairs.

The LeakBot itself is a small device which can be clipped to any pipe by a homeowner to detect leaks on the mains water supply. It then alerts customers via their smartphone to issues such as dripping taps, hidden leaks on pipes and taps being left running. The value

proposition speaks for itself, according to Craig Foster, managing director at HomeServe Labs.

"It can be mailed to a homeowner in the post and takes five minutes to install it: clip it to a pipe and push a button which connects to the Internet," he explains. "So it is cheap enough for the insurer to provide that to a homeowner for free and claim it back in reduced claims, and it keeps customers sticky by making the insurance policy tangible."

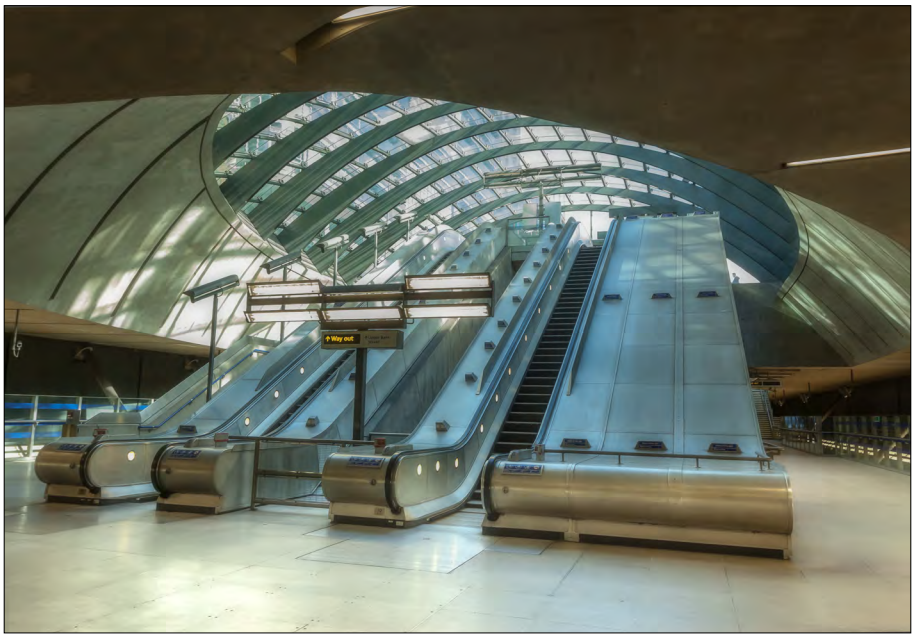
Risks

There are risks, though. IoT devices are susceptible to hacking, there are privacy and data protection issues and more recently there has been evidence that smart metres and similar IoT devices can make mistakes or even be manipulated, ending up with increased customer charges, rather than the promised savings.

Ayrdon is aware of the risks and believes transparency is key, especially with data as sensitive as that generated by a smart camera in someone's home. This is why the security of a product is a primary concern when Aviva is assessing partners in the IoT space. "If we start offering packages and recommended solutions the security of those solutions will be paramount," he says.

Foster from HomeServe Labs sees the same concerns. He recognizes the concerns with IoT devices being harnessed by hackers, but says the LeakBot doesn't have this issue.

"We use a wide area Sigfox network, so no open port to the cloud," he explains. "It's almost a cellular network, so we don't have those same hacking risks that you get when connecting to the Internet." **Scott Carey**



Credit: iStock

KONE turns to cloud to help manage its products

KONE picks Salesforce and IBM Watson to manage its intelligent network of escalators and lifts

Finnish escalator and elevator manufacturer KONE was born as a subsidiary from Helsinki-based electric motor manufacturer Strömberg in 1910. Now it operates over 1.1 million units worldwide, and has turned to IBM Watson IoT and Salesforce to manage its enormous operations, used by as many as 1 billion people every day.

Antti Koskelin, KONE's CIO, tells us that the business is moving towards something called "dynamic dispatching" – by combining intelligent analysis from IBM Watson IoT with Salesforce's Service Cloud Lightning and Field Service Lightning tools, the company will be able to respond to emergencies as they happen.

KONE has come a long way since it first started manufacturing and installing its own elevators in 1918 with a total of 50 employees. Today it's the fourth largest manufacturer of elevators and escalators in the world, and it pulls in billions of Euros in revenue a year while employing more than 50,000 people.

"If we have an urgent call from a customer, for example, someone is trapped in an elevator, or the elevator is saying something will happen if it's not maintained in the next day or so, we can dynamically schedule our 20,000 service technicians around the world," explains Koskelin.

He points to two hypothetical examples that might need maintenance at the same time – a hospital in central London and a residential student building.

"Both of these customers are calling us and saying there's someone trapped in the building, we need your help – which would you prioritize? Naturally the hospital, I would say. So if it's a hospital where the reaction time is counted in minutes, not in hours, what we'd do is look immediately to see who the closest service technician is, and who can go there immediately to serve it."

A more benign example would be a broken down lift in a residential block. Using the combination of the Salesforce field service platform and information sent by IBM's IoT sensors, KONE could look up the elevator online. By checking that nobody's inside and that it's

safely parked at the ground level, the maintenance call would be prioritized accordingly – or if there was a scheduled service technician appointment there booked for the following day, this worker would be automatically equipped with all the new information about the elevator.

Currently, KONE is using a mixture of custom and legacy technology across EMEA, Asia and the Americas, and Koskelin says this initiative is part of a wider digitization program. The Salesforce Service Cloud Lightning and Field Service Lightning will aim to bring together all of KONE's customer service agents out in the field and on the phones, with real-time service data provided by IBM IoT. The cloud service will be fully operated by Salesforce.

The project is only in its initial design phase but should be rolled out in two territories by the end of this year. Salesforce is working with KONE, along with a few other selected pilot customers, to develop the field service from the ground up.

"This is a very new solution that doesn't exist in Salesforce yet," Koskelin explains. "Salesforce is building this partly based on our needs, and partly on a few other customers' needs – so in a way, this is kind of a joint project together with Salesforce to support the business for the next decade or so."

Koskelin says KONE opted for Salesforce because, essentially, it is a Salesforce shop already in CRM. "In 2016 we were celebrating our ten year anniversary with Salesforce, and we've been very heavily implementing their CRM solution for our sales management," he explains. "That has been a great success already. Now, this contract expands the coverage into field services. What we are planning to do is digitalize our service

business with the latest generation technology, and for that we selected Salesforce based on our extremely good experience on the CRM product," he says.

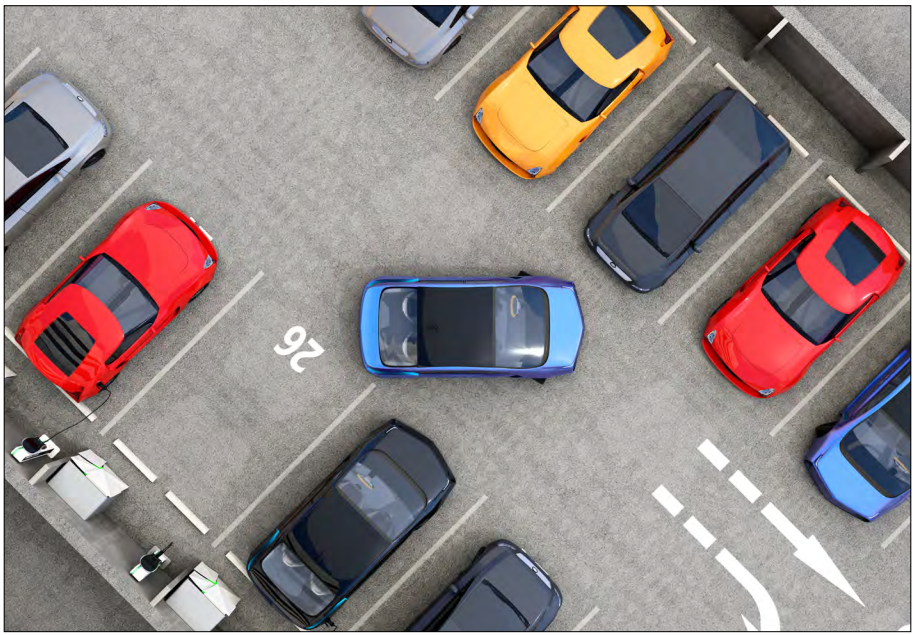
"[Salesforce] are strong partners in development overall. We feel that as we get all of our customers in the service business into one platform,that will help us provide even better services for our customers, in terms of service staff availability, availability to react to customer requests, and so on."

He adds there were other candidates for the IoT platform itself, but KONE picked IBM because the company felt confident IoT was high on its agenda. "If we look at the combination of IBM Watson analytics and then the IoT as well, this is a very good combination."

And how will Koskelin and KONE measure success? He shares two metrics: "For me as the group CIO, my main target is that we are going to get the user adoption as high as possible, and are able then to roll it out as fast as possible to the different businesses. "And another we'll follow clearly is customer satisfaction. Are we able to provide better services for our customers? To provide better proactive services for our customers, are we able to react to their needs in a better way, and send our technicians to the right customers at the right time?"

For now, KONE is recruiting into its technology and IT department, looking for talent with the appropriate skills.

"Digitalization requires that no matter if we do all the coding by ourselves, we'll still need to have a better understanding of how to utilize this," Koskelin says. "And of course, this is a change project as well – we need to train our field technicians to be able to work with the new, more intuitive solution, and dispatch their cases in a dynamic way." **Tamlin Magee**



Credit: iStock

Smart Parking turns to Google Cloud IoT Core

The parking optimization company turned to Google to bring its third generation IoT platform to life

Smart Parking is using Google's new Cloud IoT Core platform to reinvent the parking experience through use of sensors and advanced data analytics. The company helps customers including Transport for London, the City of Westminster and Hilton Hotels optimize parking at their sites through vehicle detection sensors that monitor the occupancy of spaces.

These devices generate a vast volume data that can provide increasingly sophisticated insights to businesses and drivers. To cope with the growing quantity of sensors and data and take advantage of the latest developments in data analytics, Smart Parking needed a management platform, and turned to Google's Cloud IoT Core.

"Now we have a platform that is totally secure," says John Heard, Smart Parking's CTO. "It scales from zero to a billion devices on demand and we can place it in any region to regionalize the data that's available."

The IoT market

Cloud IoT Core was developed by Google to help businesses in sectors such as utilities, transport and logistics, oil and gas and manufacturing manage their expanding fleets of smart devices and the volume of IoT data they produce, securely, at scale and from a central location. This data can then be queried using Google's own range of advanced analytics services.

Smart Parking was one of the early adopters of the platform, which was launched to the public in September. The result has made major efficiency savings for the company. "It would typically take two to three weeks of configuration and operational acceptance testing," Heard explains. "It's now taking us about three to four days. "We can activate large numbers of sensors and devices very, very quickly and we can pre-stage them in our assembly warehouses before we put them on site, which previously we had to do that while we were on site."

Smart Parking can also leverage Google's data visualization and reporting tools such as Data Studio and Data Prep, and integrate new machine learning services, like TensorFlow, as they're rolled out by Google. Heard

plans to use Google's platform to provide customer's with real-time parking guidance tailored to their individual need and location.

"The opportunity is now opening up to us to achieve our mission of reinventing the parking experience, and a big part of that is using machine learning to give better guidance into the consumer's app," reveals Heard. "Those are the sort of things that are changing the whole mentality from trying to find a parking space to being guided to it automatically and conveniently in a way that will be quite transformational. And these are the aspects that we can do that we couldn't do with the old system."

Why Google Cloud IoT Core?

Smart Parking managed the earlier iteration of its platform through a combination of Windows and Linux-based servers running on the Amazon (AWS) cloud platform. Last November, the company decided to build a third generation of its platform.

"It came to a point where we recognized that if we kept just evolving the second-generation platform we weren't going to enable ourselves to exploit and utilize the benefits of what I call 'cloud nation computing', where it's completely on demand and it scales up and down dynamically," says Heard.

"What we realized was that we needed to have an information computing platform that would enable us to scale very dynamically, very much in real-time and also open up more opportunities for ourselves."

AWS and Azure, Google's arch-rivals in cloud computing, both offer their own IoT management platforms, but Google stood out due to its reputation

for innovation in data science. “We looked around at a variety of the classical ones, Microsoft, Amazon and Google, and the characteristics that very much drove my decision-making were that we wanted to push forward into the advanced capabilities of cloud-native computing.

“It was more advanced, it was more complete, and it had a comprehensive frame that would take us forward into machine learning that was quite natural compared to other providers at this present time.”

It took just a week for the company to integrate its platform and smart devices into Cloud IoT Core, launching in September. The Smart Parking team had spent 10 years developing the previous generation of its platform. The latest generation was ready in a year. Heard attributes much of their speed to Google’s dynamic development environment, which allows them to constantly add new features.

“The Cloud IoT Core has been an acceleration that helped us to eliminate a whole variety of issues that we previously had to develop and manage for our infrastructure,” he says. “Now I can focus a team on other things.” **Tom Macauley**