



SOTI[®]

ENTERPRISE MOBILITY MANAGEMENT

“Things” are taking over the internet.

The Internet of Things (IoT) is here. It has surpassed the Internet of People (IoP) in size and complexity. Soon, there will be billions of new devices and endpoints connected together to form complex business solutions that run without human interaction or awareness. In this new world of “things” talking to “things”, management and security is more challenging and more important than ever.

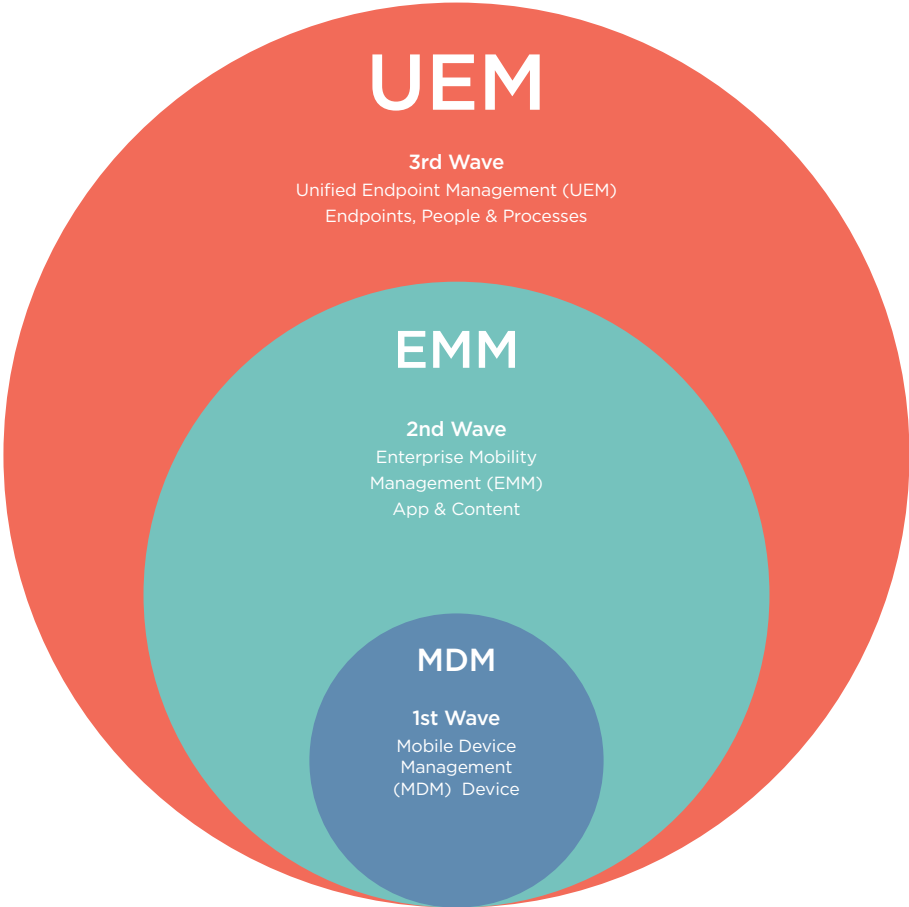
The background features a complex network of interconnected nodes and lines. The nodes are represented by various icons: a computer monitor, a shield with a star, a camera, a CD/DVD, a house with a dollar sign, a folder, a cloud, a microphone, a database cylinder, a warning sign, a key, a person icon, a prohibition sign, a microscope, a truck, a smartphone, a printer, a document, a person silhouette, a database cylinder with 'A', and a gear. The lines are a mix of solid and dashed gray.

contents

more everything

the evolution of business mobility.

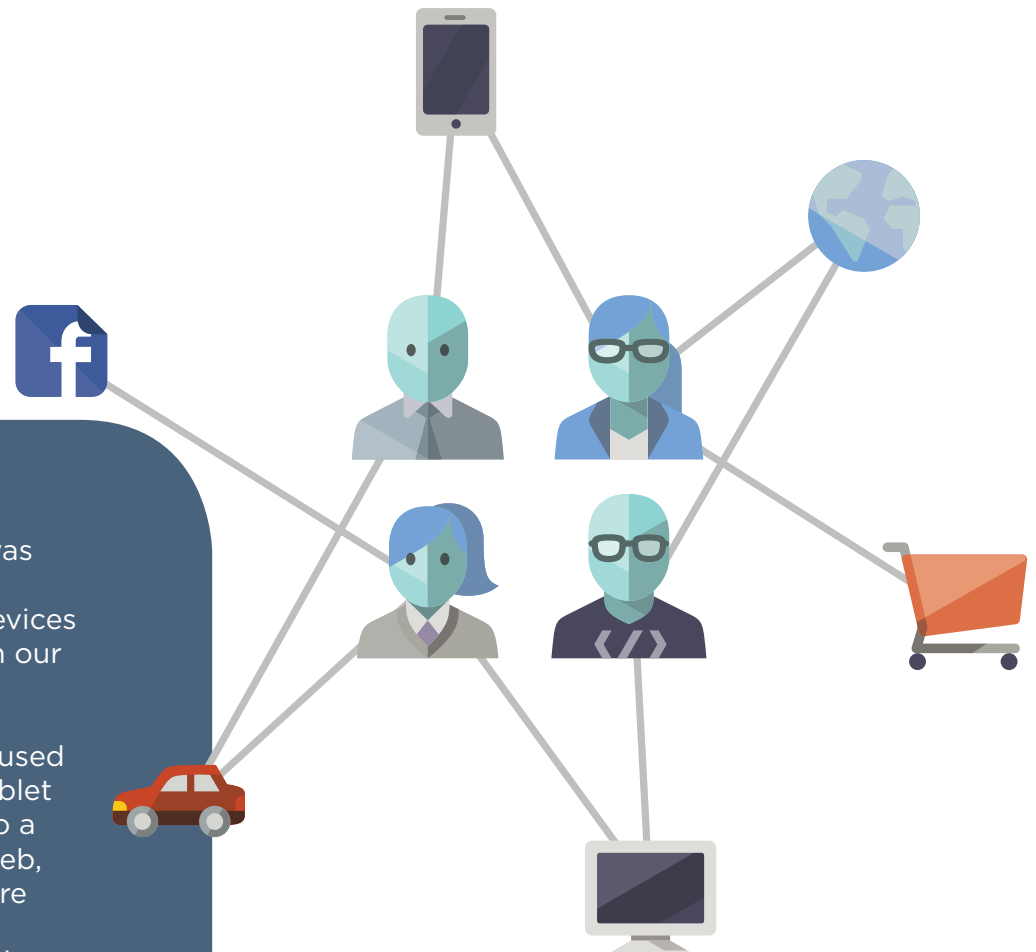
Enterprise mobility has changed significantly over the last decade. A few years ago companies were focused on deploying mobile devices to their workers to facilitate basic voice communication. Then, as smartphones were introduced and device capabilities grew, mobile applications and content became more important. Companies recognized that the smartphone was a viable application platform that could be integrated into business workflows to enhance worker productivity from any location. Now with the arrival of the Internet of Things, the market is changing yet again. In a few years, we can expect to see billions of new devices, “things,” and endpoints connected together transferring Exabytes of data to each other and to back-end systems.



the Internet of Things goes mainstream.

The Internet of Things (IoT) is not new. The concept was first introduced in 1999 by Kevin Ashton. He foresaw a future with massive numbers of connected sensors, devices and endpoints. These devices would be everywhere; in our home, our place of work and where we shop and eat.

The IoT is very different from the internet that we are used to - the Internet of People (IoP). The IoP uses a PC, tablet or smartphone running an application that connects to a remote server to get something done. Browsing the web, sending email, shopping online and watching Netflix are common examples of the Internet of People. Over the years, many new applications and even whole application categories have been launched, but the basic query/response paradigm of the IoP, and its hub and spoke topology have not changed.



from hub and spoke to massive mesh networks.

The Internet of Things is very different. It is vast networks of devices, endpoints, sensors, controllers and systems. In the era of IoT, systems of endpoints and computers can sense for themselves and use analytics and business intelligence to respond faster and better than a human. The reactions and adjustments will happen without any human intervention, and often without any human awareness.

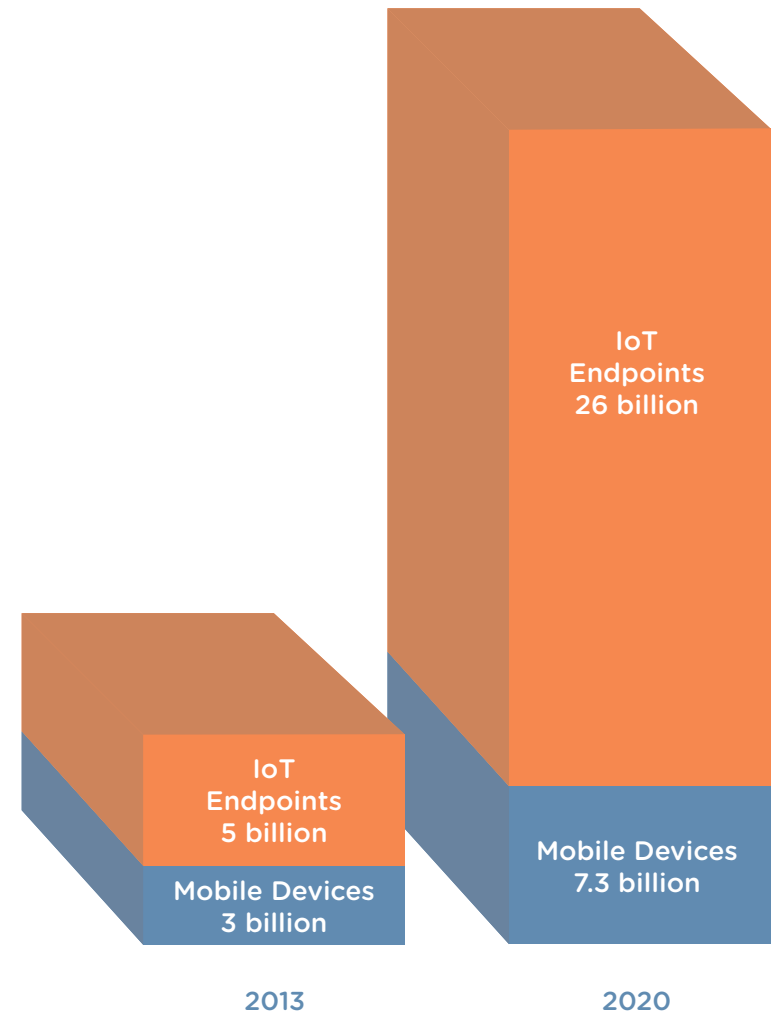
The idea of complex networks of sensors and devices operating autonomously is also not new. Smart and dumb devices (aka “things”) have been used in industrial automation and process control for decades. The ‘Industrial Internet’ uses devices that range from tiny, single-purpose sensors and pumps to large, complicated systems such as AGVs and robotics. The devices connect, communicate their status and transfer data to each other, and to controllers using standardized messaging protocols. The IoT functions almost exactly the same, but at a much larger scale and wider scope. Millions of devices, endpoints and systems connected together to deliver an automated solution.

more everything - more devices.

It is only within the last few years that the IoT has entered the mainstream and received fervent media attention and public awareness. Industry experts agree that the IoT is going to grow exponentially over the next few years. They project that by 2020, in addition to 7.3 billion mobile devices (smartphones and tablets) there will be over 26.5 billion connected IoT endpoints. Some analysts even claim there will be as many as 100 billion connected endpoints within that timeframe. Within a few years there will be 10 to 100 times more “things” using the internet than people.

26

Billion connected IoT endpoints by 2020*



Source: Gartner 2013

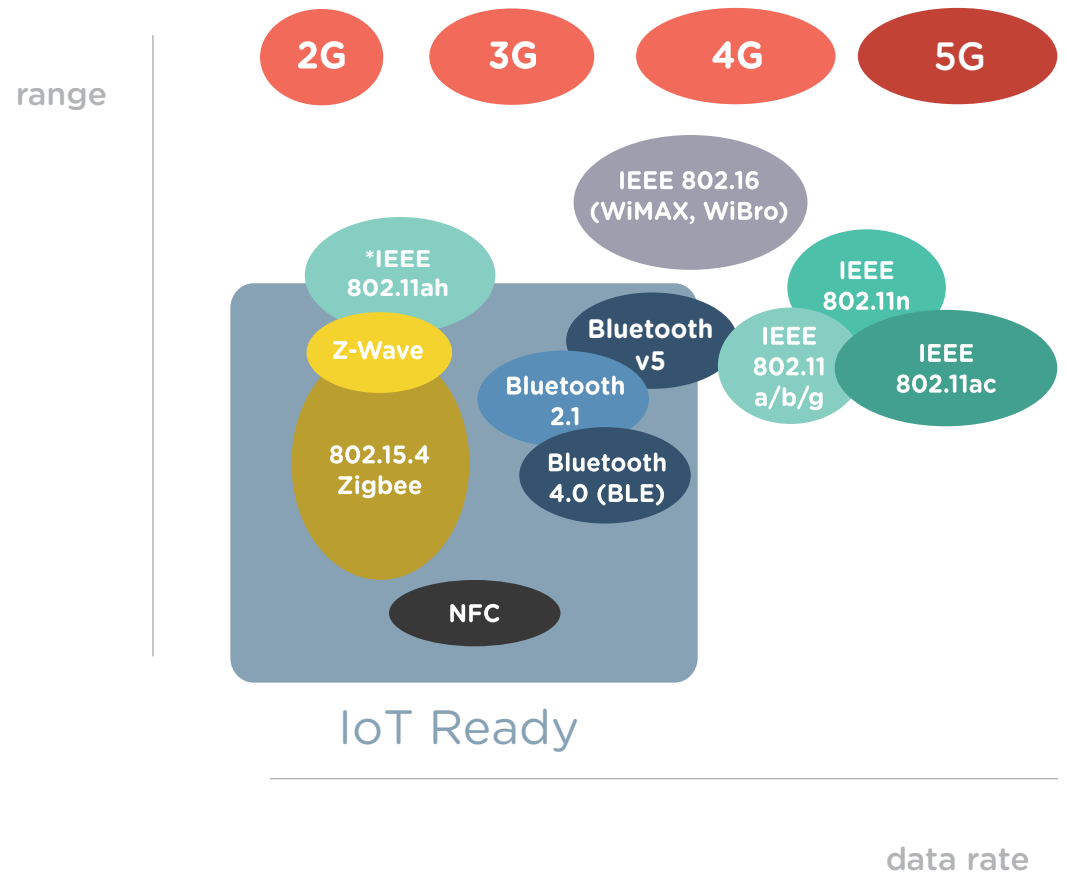
more everything - more diversity.

The IoT will see a lot of connected devices, endpoints and “things” with a diverse range of capabilities. Simple “things” like wireless sensors for temperature, pressure, light and motion; more complicated devices like digital signs, BLE beacons and wearables; all the way up to complex systems like robots, connected cars and drones. In the future, connected cars and autonomous drones will be as common as the microwave in your kitchen.

Think about your smartphone – even devices from different manufacturers have very similar features and functionality. They include screens, speakers, microphones, radios (4G, Wifi Bluetooth, NFC), batteries, cameras, and storage that work together to run apps, send messages, browse the web, etc. Now compare the features and functions of your smartphone with a temperature sensor, or an industrial robot – not very similar.

more everything - more networks.

The IoT will also see increased complexity in the area of wireless communications. Over the last several years, we have connected to the Internet of People via WiFi and cellular (2G, 3G & 4G). These wireless wide area network (WAN) protocols offer the best range, data throughput and power consumption for the everyday use of smartphones and tablets. However, most of the new IoT endpoints require 'IoT-Ready' network technologies that are optimized for low power devices that need to operate for years without replacing the battery. Bluetooth 4.0 (BLE), Bluetooth 5.0, and new network technologies based on the IEEE 802.15.4 standard have been designed for constrained devices, smaller payloads and relatively short range networking.

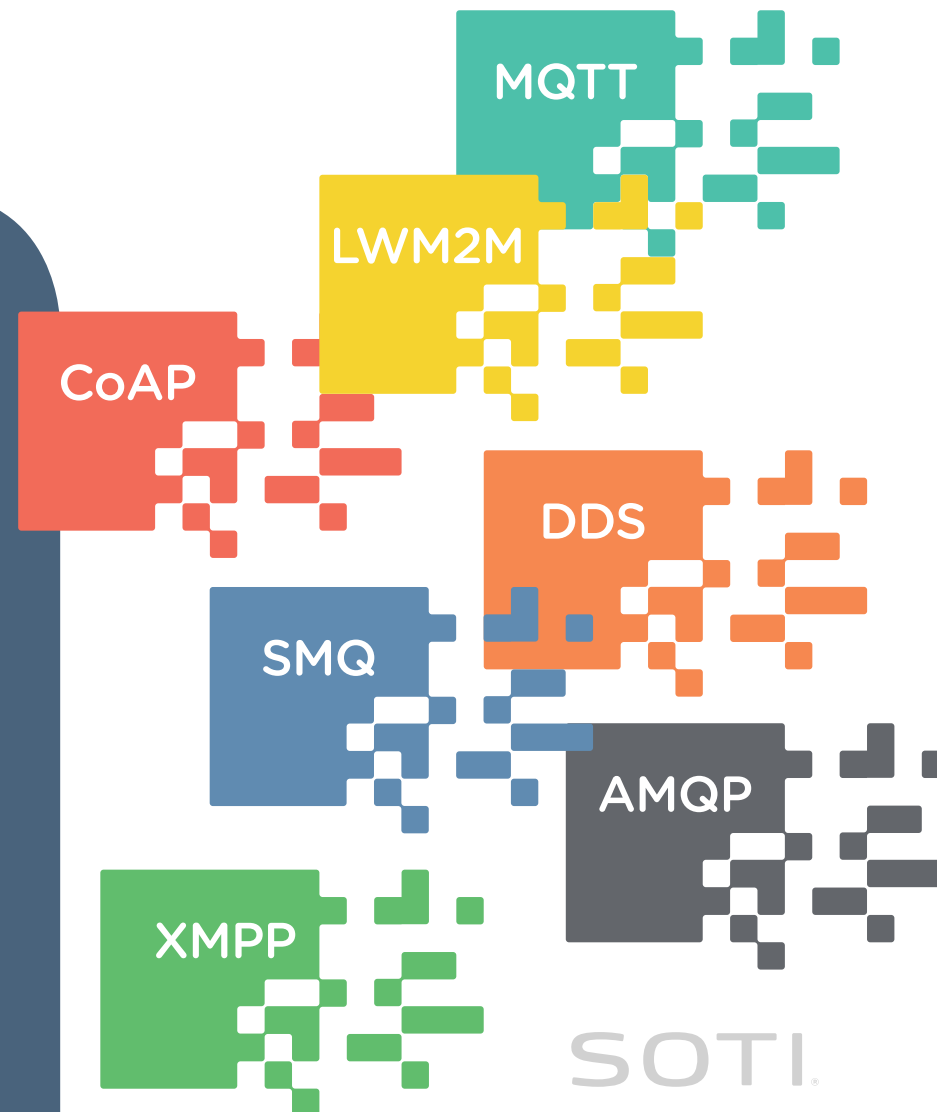


more everything - more protocols.

In addition to new networking technologies, the IoT is seeing an explosion of new standards and messaging protocols optimized for constrained devices and networks. They produce a much smaller data overhead; tens of bytes as opposed to the hundreds or thousands of bytes used for conventional web application traffic via HTTP(s), DASH and SMTP/POP/IMAP etc. It is likely (hopeful) that over the next few years, there will be some consolidation or attrition of IoT standards. However, in the interim, some of the most popular protocols to investigate are:







- MQTT (Message Queuing Telemetry Transport)
- CoAP (Constrained Application Protocol)
- LWM2M (Lightweight Machine to Machine)
- XMPP (Extensible Messaging and Presence Protocol)
- DDS (Data-Distribution Service for Real-Time Systems)
- AMQP (Advanced Message Queuing Protocol)
- SMQ (Simple Message Queue)

* [Click icons for more information](#)



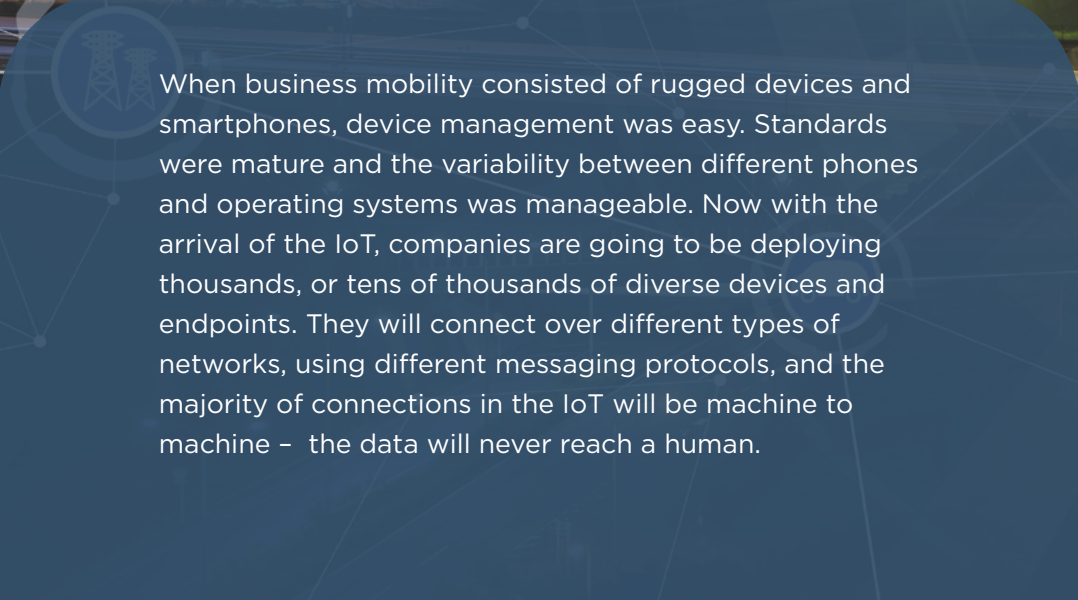
more everything - more machine to machine.

The Internet of People was mostly hub and spoke connections, or a star topology, where many clients connected to one functional server which could comprise numerous physical servers. The IoT will see many more endpoints connected to each other point to point and in a mesh. Each device, endpoint or “thing” will communicate; one to one, one to many and many to many, and they will communicate machine to machine, machine to person or person to person.

	 One to One	 One to Many	 Many to Many
 Person to Person (P2P)	Normal conversation, email, chat, SMS	Presentation, speech, broadcast, webinar, article, RSS, blog, surveys/polls	Social media, commodities, trading, cocktail party, torrents
 Person to Machine (P2M)	Games, geo-fencing, personal alarms/alerts	MMO/Coop games, creating software and applications, security alarms	e-voting, search engines, Netflix
 Machine to Machine (M2M)	Thermostat/boiler, sensor/pump, ie. continuous glucometer and automated insulin pump	Automatic security lockdown, nuclear reactor scram	IoT Ready Smart garbage cans to smart garbage trucks, anemometer, report wind conditions to airplane

The background features a night-time cityscape with illuminated buildings and streets. Overlaid on this is a network diagram consisting of white lines connecting various nodes. Several circular icons are scattered across the image: a blue atom symbol in the top left, a blue smartphone icon in the middle left, a blue Wi-Fi signal icon in the center right, a blue microscope icon in the top center, a blue gear icon in the top right, and a blue factory icon in the bottom right. A large blue banner at the top contains the text 'bringing it all together.'

bringing it all together.

A blue rounded rectangular box is positioned in the lower-left quadrant of the slide. It contains a paragraph of white text. The background of the slide is a night cityscape with a network overlay and various icons.

When business mobility consisted of rugged devices and smartphones, device management was easy. Standards were mature and the variability between different phones and operating systems was manageable. Now with the arrival of the IoT, companies are going to be deploying thousands, or tens of thousands of diverse devices and endpoints. They will connect over different types of networks, using different messaging protocols, and the majority of connections in the IoT will be machine to machine - the data will never reach a human.

top five considerations for managing the IoT.



Even for IT professionals, the IoT can be a bit intimidating. It is going to be bigger, more complex and complicated than the internet that they are used to. The IoT is creating new challenges around scale, interoperability, security and management.

What are the most important issues that companies need to consider when planning for the IoT?

- ✓ **Economies of scale should apply** - managing ten thousand devices should be just as easy as managing ten devices.
- ✓ **Device diversity is an opportunity, not a challenge** - Embrace the new devices and endpoints as they offer the potential to transform your business.
- ✓ **Security by design** - Consider the potential risks of your IoT deployment during the initial stages - plan for the worst and hope for the best.
- ✓ **Avoid proprietary ecosystems** - Open standards are not always better, but consider the long-term ramifications of locking-in to a closed ecosystem.
- ✓ **Future-proof your investment** - The IoT is just taking off and new standards and protocols are showing up every month. Don't be left behind.

The IoT has the potential to change the way your business works. You need to embrace this change, because if you don't, your competitors certainly will.

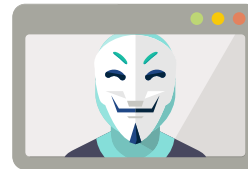
security is more important than ever.



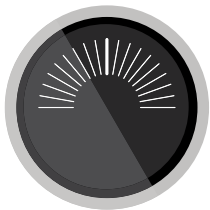
Over the next few years, as the IoT explodes and new devices and endpoints enter the marketplace, security becomes more important than ever. The scope and potential of the IoT will see millions of new endpoints being used in business. Unfortunately, for many of these new devices security was not a consideration during their design and is only being considered reactively as issues are identified in the field.



Wearable devices and smart watches with accelerometers and gyroscopes can be blue-jacked and hand/arm movement analyzed to detect door and ATM PIN codes at almost 80% accuracy.



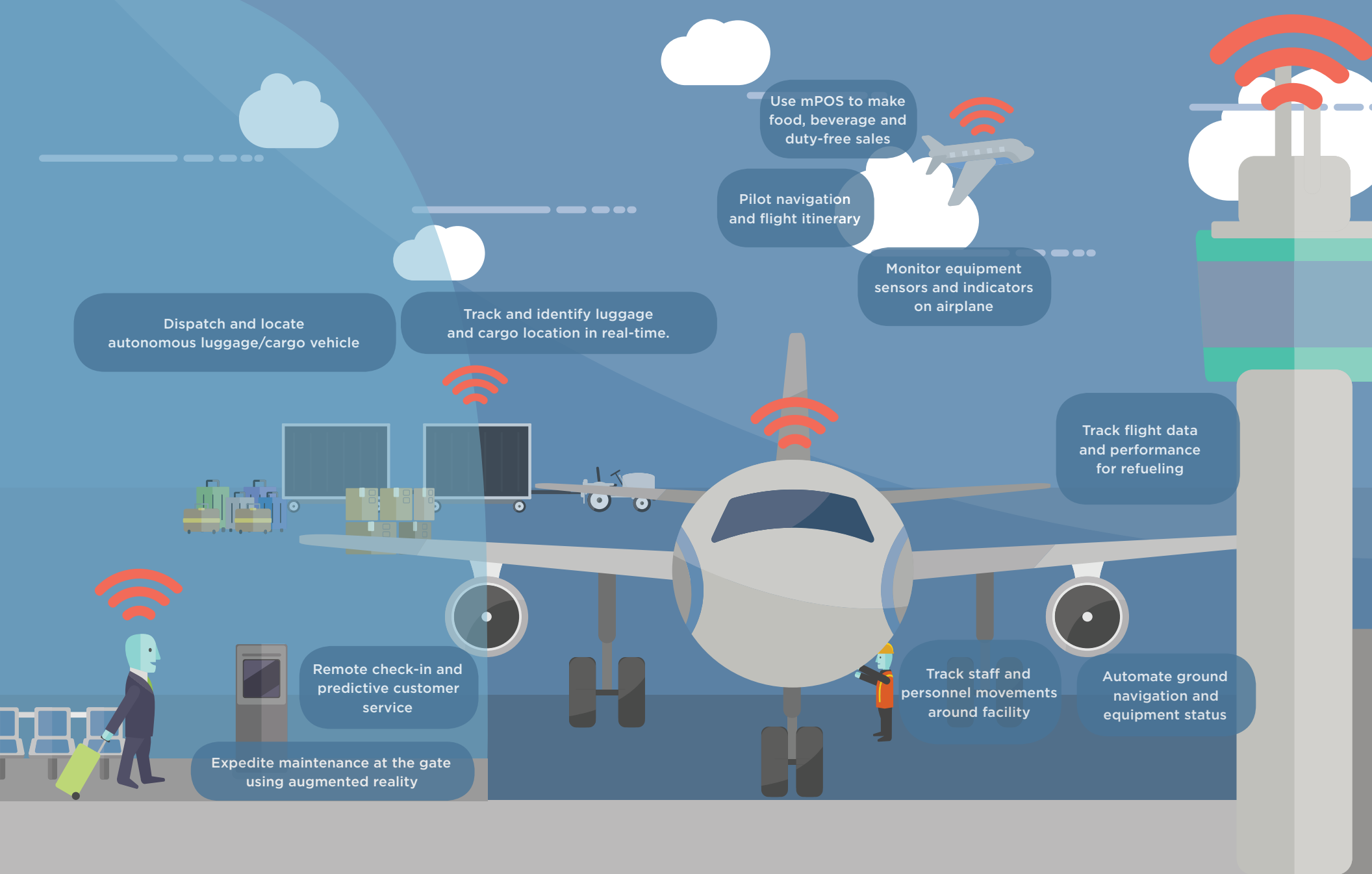
Increasingly, non-secure IoT endpoints are being hacked and co-opted as bot-nets in Tera bps DDoS attacks against internet infrastructure companies, security organizations and key government services.



A popular smart thermostat has been found to be rootable and hackable; easily becoming a client on a botnet. Equally as disturbing, configuration information, usage statistics and location information is transmitted in the clear to the company's cloud, telling someone where you live and when you go on vacation.



The FBI has sent out a warning that motor vehicles are increasingly vulnerable to remote exploits. Using on-board wireless, Bluetooth or WiFi, researchers were able to hack into vehicle electronic control units (ECU) and manipulate the vehicle remotely, including shutting down the engine, disabling the brakes or overriding the steering.



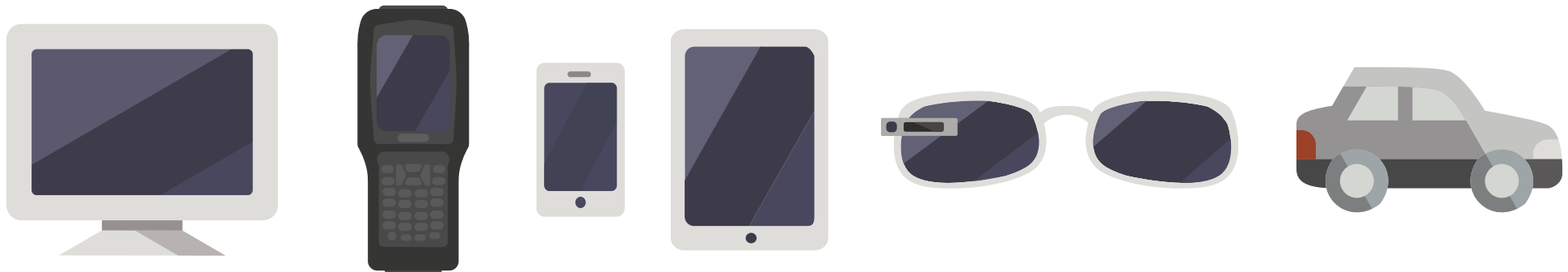
IoT in the air.

Many industries have embraced the potential of the IoT, and none more so than the airlines. They are integrating mobile devices and endpoint into their workflows to improve customer service, streamline operations, and reduce costs.

SOTI secures and manages the IoT.

As a pioneer in the Mobile Device Management (MDM) industry, SOTI managed companies special purpose mobile devices before smartphones were even introduced. Then as mobile application and content became more important, SOTI expanded their solution to deliver Enterprise Mobility Management (EMM) - to secure and manage all of these important enterprise assets. Now, SOTI is leading the way to Unified Endpoint Management (UEM); securing and managing all of the new devices, endpoints and things that are arriving with the IoT.

SOTI is committed to making your adoption of the IoT as painless as possible. SOTI's R&D is focused on understanding the IoT and how it impacts our customers now, and in the future. We make it easy for companies to use the IoT to transform your business and create endless possibilities.



SOTI.

the IoT requires Unified Endpoint Management (UEM).

SOTI has managed mobility for two decades.

SOTI managed purpose built mobile devices before smartphones were introduced, and now we are leading the way to UEM. Mobile devices, IoT endpoints and connected peripherals empower workers and allow the company to transform their business and create endless possibilities. SOTI is uniquely positioned to secure and manage the company's mobile devices and IoT endpoints to empower employees and streamline operations.

170+ Countries

2000+ Partners

16k+ Enterprise Customers

20+ years Experience Managing Mobility



Millions
of Devices Managed