gemalto
security to be free

A Safer Internet of Things

Gemalto's Guide To Making the Internet of Things A Safe Place To Connect

Harnessing the Second Digital Revolution

The Internet of Things (IoT) is set to make a greater impact on society than earlier digital revolutions. As with all new technology there are challenges – with IoT, breaches of security and privacy have the potential to cause most harm. This is why devices and data need security by default.

CONTENTS

Source: Gartner

The world of possibilities depends on trust

Imagine a future where connected devices surround us, saving time, boosting our wellbeing, improving our health and making our workplace more productive.

From Amsterdam to Zanzibar, connected devices will be transforming the world around us. Improving the efficiency of our homes, making our roads safer, encouraging us to live a more active lifestyle.

IoT builds upon the mass adoption of the Internet, mobility and social media technologies, and is fuelled by a need to make our world a more productive, healthier and safer place to live. Consumer device and industrial equipment manufacturers, automotive firms, service businesses, network and software developers are constructing a vast IoT ecosystem populated with smart, connected devices. Manufacturers from a wide array of industries are attracted to the potential of IoT to address key business consumers, including:

1. Cut the costs of delivery or maintenance of an object. General Electric, for example, uses IoT for predictive maintenance in jet engines to predict faults before they grow into big ones. Tracked flight data is also used with the goal of cutting fuel costs and improving efficiency.
2. An opportunity to create new revenues from value-added-services (VAS) and innovative business models like Product-as-a-Service (PaaS). Rolls Royce's Power-by-the-Hour approach, for example, allowed operators to pay a fixed sum per flying hour rather than paying for the engine up-front.
3. Improve the customer relationship, particularly for manufacturers who traditionally have no relationship with users once a device has been sold. Intel, for example, is adding 'brains' to vending machines which will enable vendors to add 2 for 1 offers, discounts and loyalty programs to increase sales.

Building trust

Whether it's to cut costs, generate new revenues or have a better understanding of customers, the business model only works when there is trust between the user and the supplier.

From a user's point of view, trust depends on a number of factors such as the reliability and availability of connectivity. From a supplier's point of view, they need to trust that the investment they make in a connected device can be recovered (revenue assurance).

But perhaps the most significant aspect of trust relates to data privacy and security. Developers need to consider the complete journey of that information when designing their connected devices.

> "The digital shift instigated by the Nexus of Forces (cloud, mobile, social and information), and boosted by IoT, threatens many existing businesses. They have no choice but to pursue IoT, like they've done with the consumerization of IT,"
>
> **Jim Tully, vice president and distinguished analyst at Gartner** [1]

Secure interfaces must be built into things

Data in motion will travel from a host of devices, through diverse networks to different data centers located in the cloud.

IoT will not reach its full potential unless users can trust that their connected devices are secure and their privacy is guaranteed. Therefore, data must be secured not only on the device, but on its journey through the network towards the data center and beyond. With so many links in the chain, the security framework must be interconnected and coordinated to avoid breaches, snooping, hacking or accidental leaks.

1 IN 5

VEHICLES ON THE ROAD WILL HAVE SOME FORM OF WIRELESS NETWORK CONNECTION BY 2020, AMOUNTING TO MORE THAN

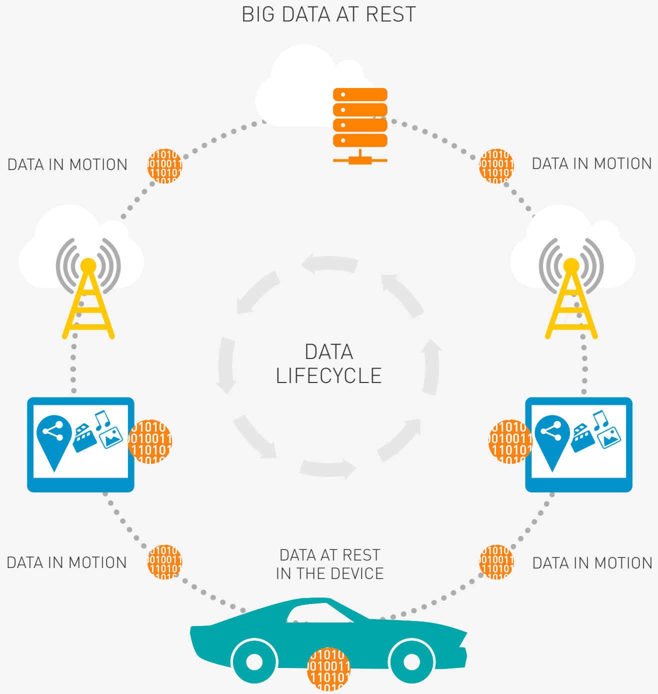
250 MILLION

CONNECTED VEHICLES WORLDWIDE Source: Gartner

One of the major considerations with IoT is that an object – be it a car, a smart meter or a health monitor – will suddenly become part of a networked environment. Some IoT devices will run our critical infrastructure, such as water, electric, public health and transportation, which will make them a potential target for industrial espionage as well as denial of service (DoS) and other hack attacks. Personal data – perhaps financial records or location history – residing on networks will be an obvious target for cybercriminals.

Data in motion must be secured every step of the way. Take the connected car, for example. It may have access to a personal calendar to plan the fastest route to the next meeting. To send information from the in-car navigation and entertainment system, provided by the manufacturer, there must be a wireless connection provided by a service provider. Information is downloaded or sent via a system in the cloud. Basically, a "thing" requires the Internet and cloud to be truly connected to let data flow from one place to another.

DATA LIFECYCLE FOR THE CONNECTED CAR



Data within an IoT ecosystem is either in motion or at rest. Data at rest is the one that resides within the device or the cloud, whereas data in motion is the data moving from one node to the other. Driving data, for example, could be at rest in the car computer or sent over the cellular network to the cloud for fuel consumption analysis. Conversely, media could be streamed from a cloud server to the in-car digital console.

Protecting our privacy

Tempted by the array of data that is collected from smart devices, cybercriminals could find new ways of entering our lives, our homes and our privacy.

Privacy, security and trust cannot be an afterthought when designing for IoT. After all these things, in some cases, are collecting highly personal information. Security needs to be baked in from the very beginning to manage this information in motion and control who has access to it.

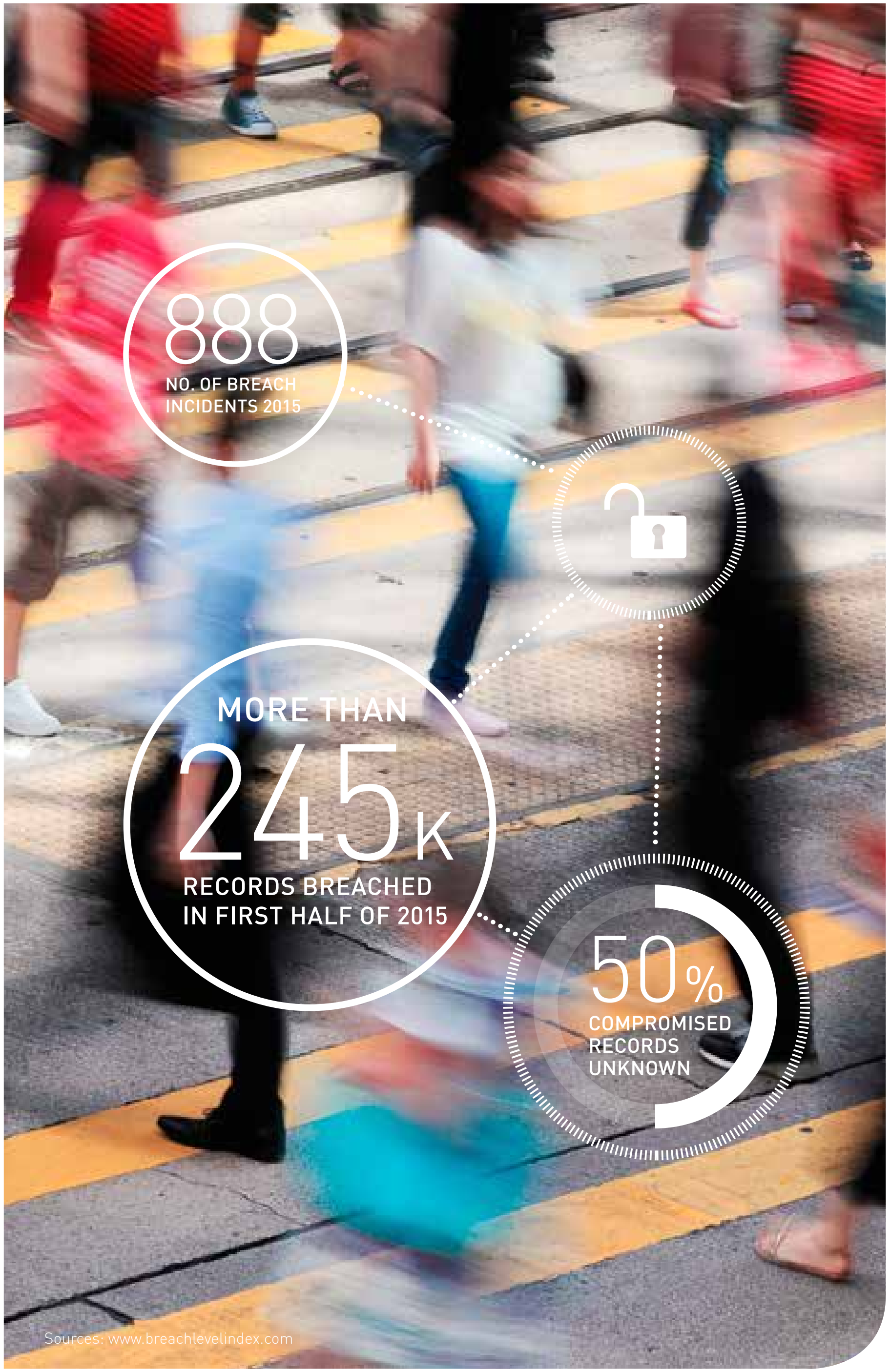
Consider the 2015 Foscam baby monitor hack. A family which used a wireless Foscam IP baby monitor were hacked.

> The hacker took control of the camera and moved it around, following the mother whilst talking to her and making comments about her child.[2]

This example spotlights the importance of consumer privacy when it comes to the connected world of IoT, where dishwashers can come on automatically when the grid is at its lowest and cars can call emergency services following an accident. Much of the data companies hold about us has, until now, been explicitly and voluntarily provided.

But increasingly data collected and transmitted goes beyond personally identifying information and creates a detailed pattern of our everyday lives.

Take for example, the smart meter. It collects telemetry data for the utility company which owns the device, which is analysed to build up a picture of how energy is used. From the consumer perspective, it creates a record of activity within the user's own home. This data in the wrong hands provides an invitation to break-in when the homeowner is away.


888
NO. OF BREACH INCIDENTS 2015
MORE THAN
245K
RECORDS BREACHED IN FIRST HALF OF 2015
50%
COMPROMISED RECORDS UNKNOWN

Sources: www.breachlevelindex.com

A double act: privacy and authentication

Ensuring the users are who they say they are and authorised to use the device is the essential first step in securing a device.

Authentication is essential with connected devices. For instance, when we go to unlock our connected car with our mobile phone we want to know that no-one else can unlock it.

But cars are not always as secure as you think! Australian security researcher Silvo Cesare has demonstrated a security flaw in car locks that enables him to disable the alarm and get into the car without leaving any evidence behind for police. He uses a simple software defined radio and an antenna to capture and transmit wireless signals to gain entry. [3]

ORGANIZATIONS TAKE AN AVERAGE

46 DAYS

AND CAN SPEND UP TO

$2 MILLION

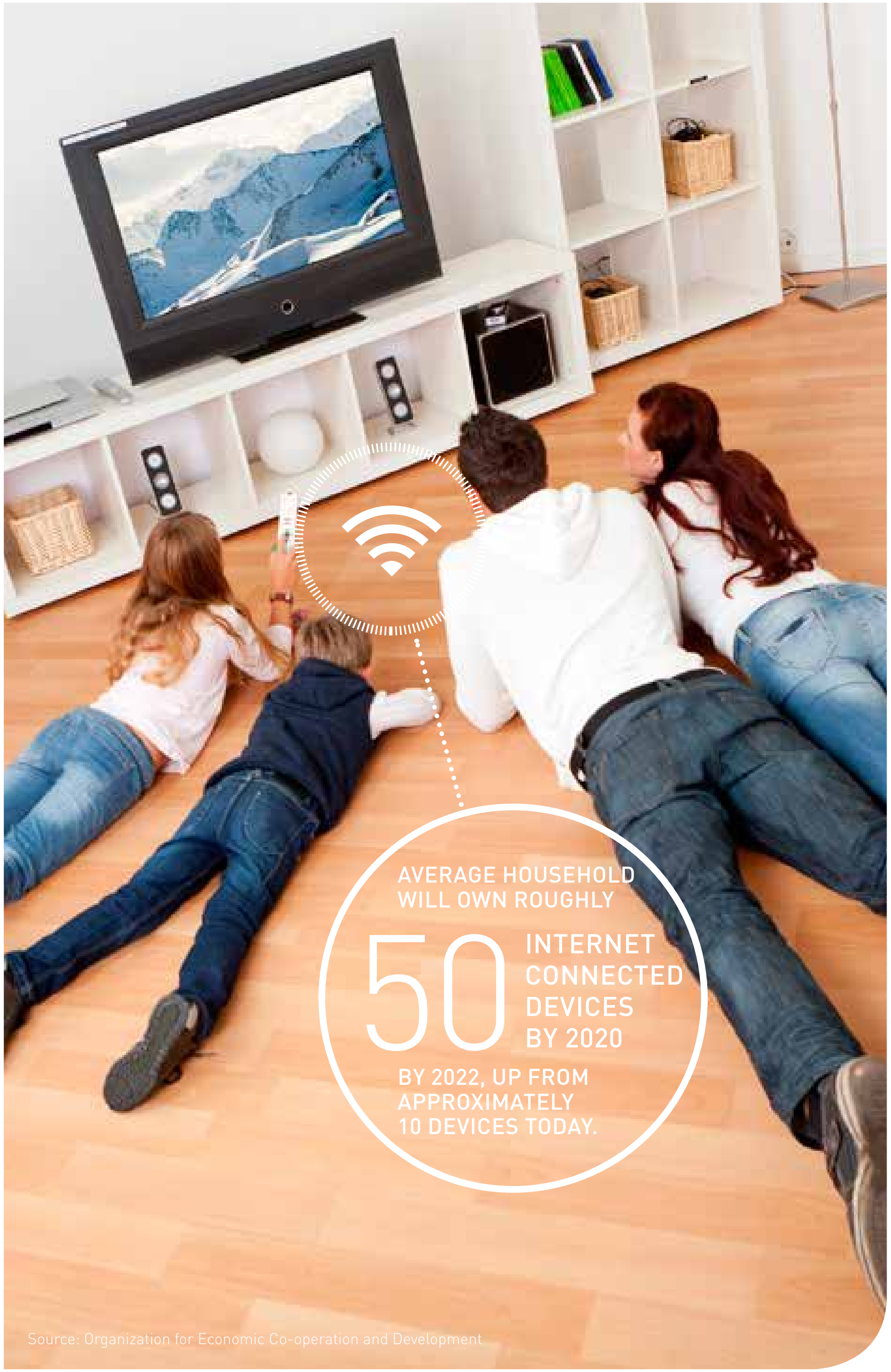
TO RECOVER FROM A CYBERATTACK

(2015 Ponemon Institute of Cyber Crime Study)

> “Consumers are starting to pull away from brands that have been breached and they’re becoming aware that there’s a thriving market in more durable identity credentials than just credit cards.”
>
> **Christian A. Christiansen, IDC Program Vice President, Security Products and Services**

Suppliers must also be authorised to access a remote device. Electric vehicle developer Tesla notifies drivers that an upgrade to its firmware is available and when it will be downloaded. This shows the driver that the upgrade has come directly from Tesla and not someone hacking into the system.[4]

To further enhance authentication, biometric data such as fingerprints and iris scans are increasingly being used to prove who we say we are.


AVERAGE HOUSEHOLD WILL OWN ROUGHLY
50
INTERNET CONNECTED DEVICES BY 2020
BY 2022, UP FROM APPROXIMATELY 10 DEVICES TODAY.

Source: Organization for Economic Co-operation and Development

Threats are unavoidable

With huge amounts of information being generated by connected devices, the focus must shift to protecting data that is meaningful.

The first step in creating a security framework is recognising the types of threat. Here are some examples of key threats:

Phishing

The fraudulent practice of sending emails pretending to be from a reputable company in order to entice individuals to reveal sensitive information such as credit card numbers.

App hacking

The low hanging fruit in the hacking world. There are automated tools easily available on the market and lots of them are free. Unlike centralized Web environments, apps exist in an unregulated mobile device ecosystem. Unprotected binary code in mobile apps makes them fast and easy to modify and exploit. Binary code is the code that devices read to make an app work. It is basically what you download when you access mobile apps in an app store such as iTunes or Google Play.

DOS attacks

Denial of Service attacks are designed to temporarily or indefinitely crash a network. Fixes are available, but like viruses, hackers are continually thinking up new ones.

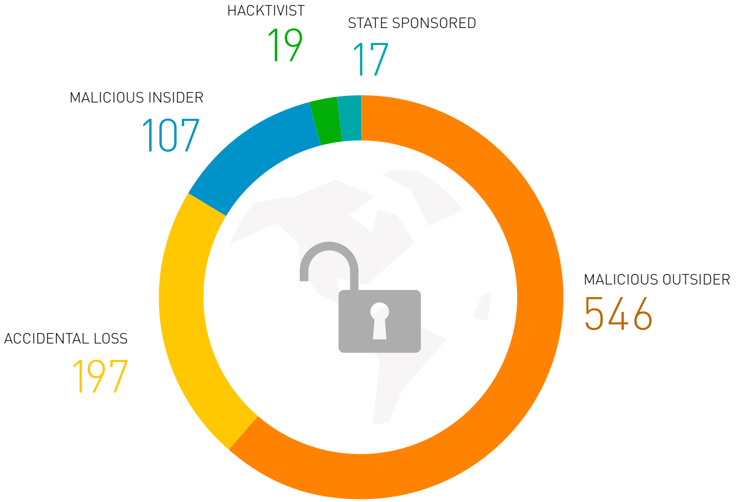
DDoS attacks

Distributed Denial of Service attacks are designed to make an online service unavailable by flooding it with traffic from multiple sources.

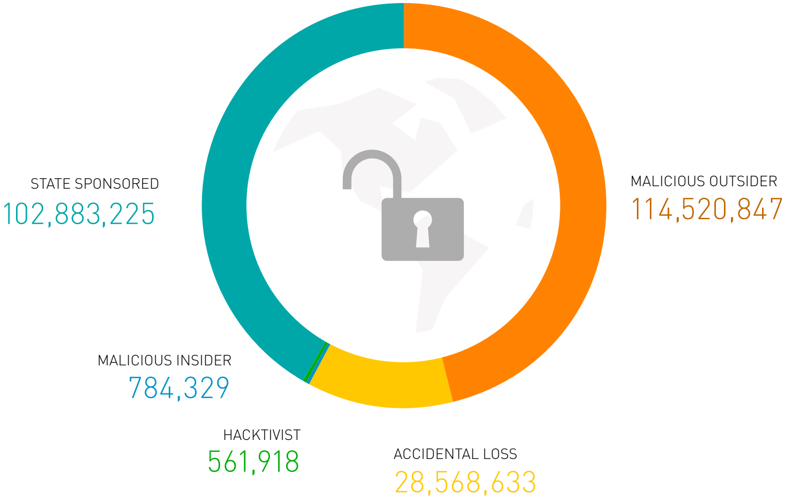
Physical intrusion

Hacking normally happens remotely. But a physical intrusion is when a device and its components are actually tampered with.

Number of breach incidents in 2015



Number of records breached incidents in 2015



Sources:Breach Level Index (Gemalto)

Every device you can think of can be hacked

The more devices and points of entry there are on a network, the more opportunities there are for cybercriminals to sneak in.

Virtually every connected device from smart TVs, fitness devices and home security to printers, in-car systems and networked lightbulbs, has been hacked at some point.

IoT is unprecedented in its capacity and scale. To accelerate innovation and acceptance, information between the device, the network and the cloud must be as secure as possible in the face of growing security challenges. Building security into the IoT ecosystem makes authentication a straightforward, frictionless process for the consumer.

8000 PEOPLE

WERE HACKED WHEN AN ANONYMOUS GROUP HACKED INTO THE EUROPEAN SPACE AGENCY AND LEAKED THE NAMES, EMAIL ADDRESSES AND PASSWORDS WHICH WERE POSTED IN THREE DATA DUMPS ON JUSTPASTE.IT.

University of Central Florida researchers demonstrated how easily a Nest Learning thermostat can be compromised if a hacker has physical access to the device. Within 15 seconds, a hacker can remove the Nest from its mount, plug in a micro USB cable, and backdoor the device without the owner realising. The compromised Nest can then be used to spy on its owner for example, attack other devices on the network or steal wireless network credentials.[5]

Symantec used customised Rasberry Pi computers to draw attention to glaring security holes in fitness trackers. The security experts found that some devices could be easily tracked geographically.[6]

Security experts Proofpoint found that an Internet connected fridge helped send more than 75,000 spam and phishing emails over the holiday break in 2014.[7]

Hacker and security expert Chris Roberts of One World Labs in Denver, US, hacked into a plane's in-flight entertainment system and made it briefly fly sideways, according to an FBI Search warrant filed in April 2015.[8]

A hi-tech signalling system that is destined to control all of the UK's trains could be hacked into potentially causing a serious incident, Professor David Stupples told the BBC. Network Rail, which is testing the European Rail Traffic Management System, acknowledged the potential threat.[9]

In-car connectivity continues to grow, but what happens when a car gets hacked. Wired reporter Andy Greenberg found out when a Jeep Cherokee he was driving at 70 mph was 'taken over' on a St Louis highway in the US.[10]

The same security researchers claimed that 471,000 connected vehicles could be hacked from nearly anywhere in the world – as long as the attacker knew the IP address of the target vehicle.

Security for the life of the device

To grow and retain trust among users, the ecosystem that supports the foundation of the Internet of Things requires a collaborative, umbrella approach to IoT security.

No single control is enough to stop an attack. A multi-layered approach has to be taken, right from when the device is switched on. It is simple – security must be addressed throughout the lifecycle of the device, from design to operation.

In addition it is essential that IoT is secured at all levels – the device itself, connection through the network and in the cloud.

> "The connected kitchen creates digital business opportunities at several levels in the food supply chain and retail food service. A real-time inventory data collection from sensors related to kitchen ingredients enables automated generation and ordering of shopping lists, resulting in a streamlined and efficient inventory and optimised supply chain management."
>
> **Satish R.M,**
> **Principle Analyst, Gartner**

Protection: where, when and how you want it

Building a protective wall around IoT will come with its challenges – these include:

- Diversity of connectivity types: there are so many ways to connect. Mobile networks, Bluetooth and WiFi have been the main connectivity method to date, but new network technologies are emerging for different use cases. These include: LoRa, UNB, PLC, shortrange BTLe, Weightless, LTE-M and ZigBee. Each new network technology brings new threat opportunities.
- Diversity of industries: With IoT covering everything from large scale industrial systems, such as wind farms to wearables, each has its own ecosystem. Security models may be different, but one thing in common they all have is the huge volume of data they will collect. The more granular the information the more sensitive it is.

Each stage, each connection adds a link to the chain. Security solutions need to snap together at different points on this chain. From the user perspective, securing IoT depends on a secure device, network and ecosystem incorporating trusted service management, data management and compliance with regulation.

The four best practices for IoT protection:

Evaluating risk – developers need to understand all the potential vulnerabilities. Evaluation processes should cover privacy, safety, fraud, cyberattacks and IP theft. Evaluating risk is not easy as cybercriminals are continually working on launching new threats. As there is no one size that fits all it is advisable to bring in a security expert at this stage.

Security by design – it is key that device security is duly considered at the development stage. This should include end-to-end points and countermeasures, including tamperproof hardware and software.

Securing the data – strong authentication, encryption and securely managed encryption keys need to be included to secure information stored on the device and in motion.

Lifecycle management – security is not a one-off process and then you can forget about it. It is imperative that IoT devices are protected for the lifecycle of the device, be it a stand-alone product or integrated into a car, for example.

THE CONNECTED KITCHEN WILL CONTRIBUTE AT LEAST 15% SAVINGS IN THE FOOD AND BEVERAGE INDUSTRY BY 2020.

Realizing the benefits of a totally connected world

Consumers will be increasingly drawn to the convenience of IoT, safe in the knowledge that it is secure. It will also enable IoT to deliver on its other promises including increased efficiencies across industries, cost savings in healthcare and energy saving in our cities.

36%

TOTAL CONNECTED SMART TV'S BY 2020

SMART TV SETS WILL ACCOUNT FOR 36 PER CENT OF THE 2020 TOTAL CONNECTED SETS, WITH 320 MILLION (OF WHICH 56 MILLION WILL BE IN THE US AND 64 MILLION IN CHINA).

(source: Digital TV Research: Connected TV forecast report)

The benefits of a secure and trustworthy IoT system to business:

Lower operating costs for business

ThyssenKrupp Elevator maintains over 1.2 million elevators worldwide, for example. Predictive and pre-emptive maintenance, bringing Microsoft IoT technologies, is guaranteeing a higher uptime on elevators and the company said it has started to see a fall in support calls. [11]

Less legal action and associated costs from data breaches

According to research by IBM and the Ponemon Institute the average total cost of a data breach to a company is $3.79 million. Shoring up security reduces risk.

More opportunity to partner

IoT will open up markets and provide more opportunities to partner. Google, for example, has been working on software that will help automakers build self-drive cars.

Business continuity

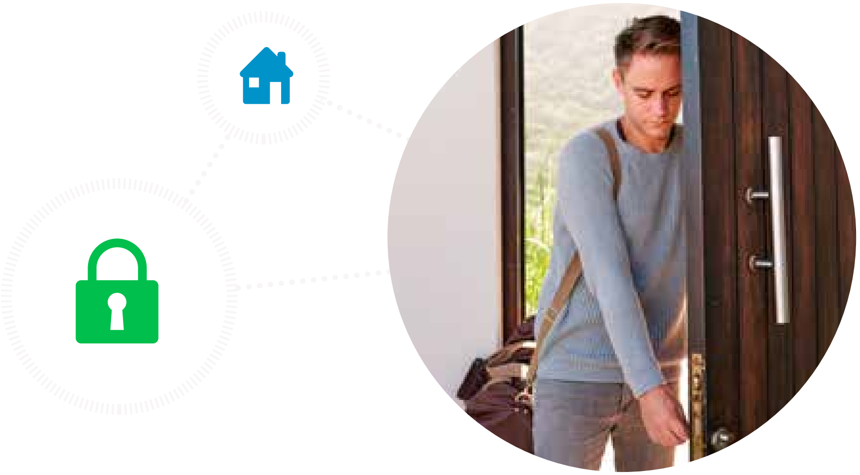
With so many ecosystem players involved (OEMs, connectivity providers, cloud service providers, ISVs etc) it is paramount that all components and steps in the ecosystem are secured to ensure there are no disruptions. Robust security ensures businesses can benefit from connected business continuity with customers.

The digital world is evolving fast and a secure ecosystem is building a safer future for IoT.

Security Inside and Out

Security at the device, network and cloud level are critical to the efficient and safe operation of IoT, protecting data in motion and at rest. Intelligence that enables devices to carry out tasks in the IoT ecosystem must also be tapped into to enable them to recognise and combat malicious threats. Here at Gemalto, we are focused on providing robust security solutions developed for the increasingly complex world these billions of connected "things" are creating.

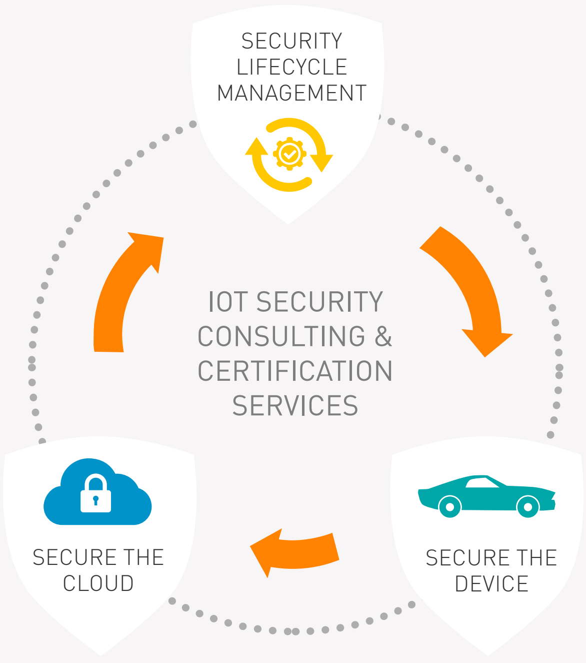
Today's innovations are only just beginning. IoT will play a pervasive role in how we live and work in the future. But the only way connected "things" will reach their full potential is with the trust of consumers. Gemalto can provide you with a worry free path to IoT adoption, ensuring you stay safe and enjoy the benefits of a truly connected world.



GEMALTO CORE OFFERS TO SECURE THE IoT

- Software Activation & Licensing
- Dynamic Key Management (for Authentication & Encryption)

- Secure Provisioning of Key Credentials & Tokens


SECURITY LIFECYCLE MANAGEMENT
IOT SECURITY CONSULTING & CERTIFICATION SERVICES
SECURE THE CLOUD
SECURE THE DEVICE

- Big Data Encryption
- Server Protection
- Cloud Application Security

- Secure Device Access
- Sensitive Data Security
- Communication Encryption
- Protect Software Integrity

For more information, please visit **gemalto.com/iot**,
or mail us at **iot.query@gemalto.com**

Sources:

(1) Gartner Symposium/ITExpo 2014
(2) Foscam baby monitor hack
(3) Silvo Cesare car lock hack
(4) Telsa firmware updates
(5) Hacking the Nest Thermostat
(6) Symantec security flaws in fitness trackers/wearables
(7) Fridges sending spam
(8) Aeroplane hack
(9) Train hack
(10) Jeep hack
(11) ThyssenKrupp elevators reduced downtime with IoT

EB (EN)-Jan.2016 – Photo credit: Shutterstock – Design: Futurity Media

GEMALTO.COM

gemalto
security to be free