TRANSFORMA INSIGHTS

Why enterprises need 'IoT Security-as-a-Service'

A White Paper

Sponsored by:

wireless logic

About this report

The rapidly evolving IoT security threat landscape necessitates enterprises finding trusted partners to mitigate risks across the end-point, network, transport, cloud/data and application layers.

This report provides enterprises with a view on the evolving IoT security landscape and the best mechanisms for mitigating the risk and impact of security threats. It starts with the results of Transforma Insights' recent IoT Connectivity Survey, demonstrating how critical security is considered to be. The following sections examine the ways in which the security threat is evolving, a dive into some of the legislation affecting IoT security, and a topology of IoT security, identifying the various types of security requirements. The final sections provide enterprises with a guide to how security considerations need to be stitched into their IoT deployments, and an explanation of why Transforma Insights believes that there is a need for something called 'IoT Security-as-a-Service' to mitigate growing and evolving IoT threats.

About the Author

Matt Hatton, Founding Partner, Transforma Insights

Matt is a well respected commentator and technology industry expert with 25 years experience at the cutting edge of technology research and consulting. He is a thought-leader in Telecommunications, Digital Transformation and the Internet of Things. He is widely quoted in trade publications and frequent speaker at conferences.

TRANSFORMA INSIGHTS

Key messages

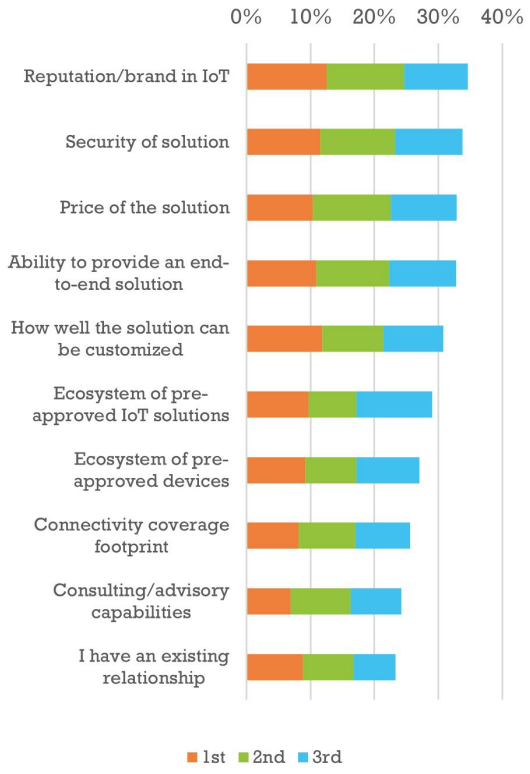
- IoT is complicated, with many moving parts spanning multiple different disciplines (e.g. device, cloud, transport, and network), all of which have their own special security considerations.
- IoT security risks are evolving fast making it increasingly challenging for enterprises to stay on top of them.
- The regulatory landscape is particularly moving fast at the moment, with new rules and regulations emerging every year.
- IoT security must consider all of the constituent parts of the solution holistically; a chain is only as strong as its weakest link.
- Enterprises must conduct due diligence on their suppliers. Your security is only as good as that of your suppliers.
- The optimum approach for many will be to find a trusted partner, delivering IoT security as a managed service.
- Enterprises will never completely remove risk. There will always be breaches. A good strategy includes serious consideration of remediation after breach.

TRANSFORMA INSIGHTS

Enterprise perspectives on IoT security

Top factors influencing choice of vendor, 1st, 2nd, 3rd choice

[Source: Transforma Insights Enterprise IoT survey, 2022]



Q8: What are the top factors that would influence you to select a particular IoT solution provider? (n=1,114)

Security continues to be one of the top requirements for enterprise IoT buyers. According to a survey conducted by Transforma Insights in September/October 2022 of over 1,100 buyers of enterprise cellular-based IoT connectivity, security was the number two factor influencing the choice of connectivity provider.

As illustrated in the chart on the left, it was 'reputation/brand' that was the top choice, indicating that there is a gating factor for vendor selection which first considers which providers are reputable and reliable before going on to consider topics such as security and price. However, security considerations would likely also be part of the thought process of determining which providers would be deemed to have a good reputation.

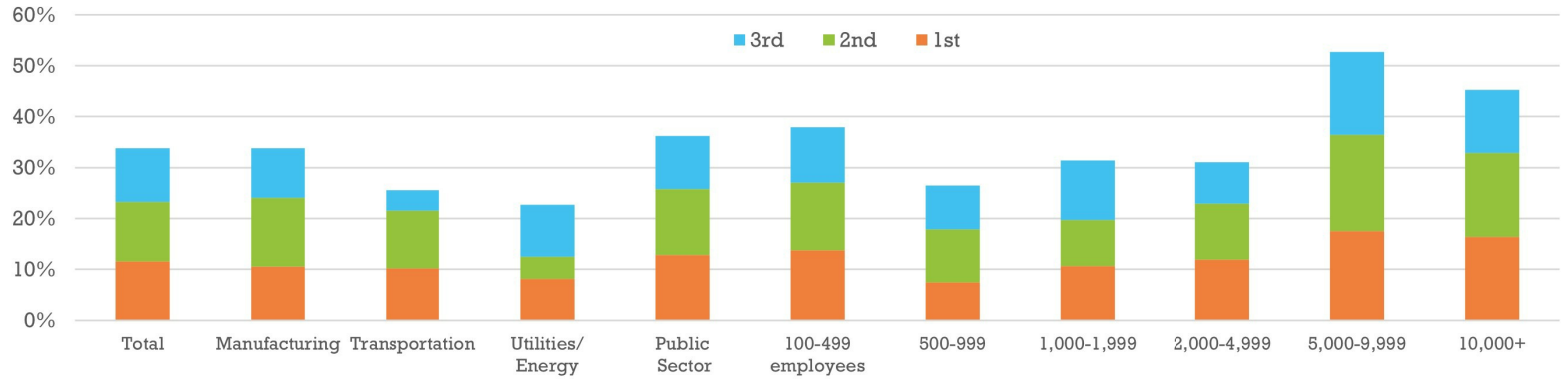
Digging into the topic of security in a little more depth, as we do in the second graphic shown below, we can see that the importance of security varies in a quite marked way depending on the geography, sector and size of the organisation.

While a total of 34% of respondents quotes security as being one of their top 3 considerations, this was as low as 23% for the Utilities/Energy vertical and as high as 36% for the public sector. The low rating in the Utilities/Energy sector is perhaps surprising given the fact that it is heavily focused on critical national infrastructure involving applications such as smart metering and smart grid. Perhaps we can interpret it that they are at this stage comfortable with the levels of security they receive and have moved on to thinking about other topics. This is somewhat borne out by the fact that when asked in a separate question about demand for future features, respondents in that sector strongly favour lower prices as a priority rather than security.

As shown in the chart, there is also something of a trend for larger organisations to have a greater consideration of matters relating to security than their smaller peers. This might well reflect the fact that larger organisations are likely to deploy more critical use cases, whereas for smaller organisations there may be fewer threats. Or alternatively it may just be that smaller organisations are more focused on just getting their IoT project off the ground.

Top factors influencing choice of vendor: Security of solution, 1st, 2nd, 3rd choice

[Source: Transforma Insights, 2022]



Q8: What are the top factors that would influence you to select a particular IoT solution provider? "Security of solution". (n= 1,114, US 510, UK 119, Germany 131, France 115, Italy 124, Spain 115, Manufacturing 237, Transport 176, Utilities 185, Public 163, Other 353, 100-499 211, 500-999 257, 1,000-1,999 290, 2,000-4,999 209, 5,000-9,999 74, 10,000+ 73)

TRANSFORMA INSIGHTS

IoT security threat landscape

The security threats associated with the Internet of Things are growing. Enterprises are paying more attention than ever to how to mitigate the growing risk. Transforma Insights identifies 10 key reasons why the threat from security breaches in IoT is increasing.

1. More use cases

There are more enterprises and consumers deploying IoT than ever before, opening up more potential hacking opportunities for bad actors. Consumer devices such as refrigerators, washing machines, ovens and lighting systems increasingly shipping with connectivity embedded. Enterprises are finding more and more ways in which IoT can be useful for streamlining business processes or giving them a competitive edge, whether that be in supply chain, manufacturing automation, retail or any other vertical.

The democratisation of the use of IoT makes for a greater number of potentially vulnerable systems and end-points. It also means that there is a great potential for losing track of legacy IoT deployments. Unlike most traditional ICT deployments, such as PCs, phones or servers, these IoT devices are usually unattended and will often be operating for decades without any need to replace them, or interact with them in any way. It's easy to lose track of every thermostat, security camera and water pressure monitoring device installed on your network.

2. Bigger scale

Hand in hand with the increase in use cases, the volumes are growing. At the end of 2022, Transforma Insights estimates that there were 13.2 billion IoT connections worldwide. By 2032 that figure is expected to increase to 34.7 billion. Simply by virtue of the growth in numbers of devices, the cyber security vulnerabilities are multiplied.

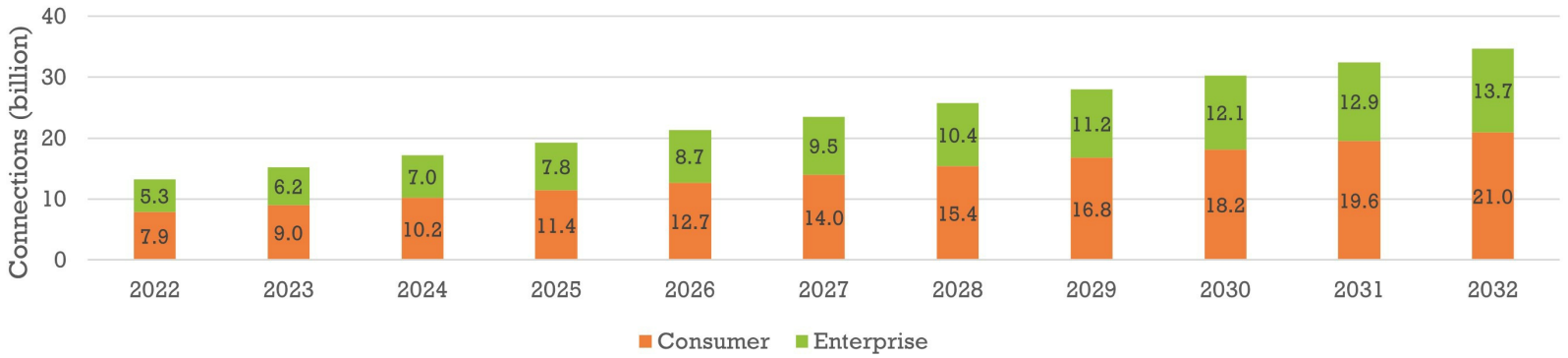
3. More mission-critical

According to a recent survey by Transforma Insights, enterprise IoT adoption is heading into a new phase whereby businesses are entrusting more critical core systems and processes, including those directly affecting their relationship with customers, to IoT .

The counterpoint to this use for more mission-critical systems is that such IoT deployments are more appealing for ransomware attacks, and more appealing to state actors looking to find vulnerabilities in critical national infrastructure. One good example here is the Colonial Pipeline hack of 2021, whereby a US oil pipeline carrying refined fuel was subject to a ransomware attack. The increasing use of remote management of such critical assets opens up the potential for attack.

Global IoT connections, 2022-32

[Source: Transforma Insights, 2023]



TRANSFORMA INSIGHTS

IoT security threat landscape

4. Physical vulnerability

Many IoT devices are located remotely and almost all of them are unattended, i.e. there isn't someone constantly interacting with them. As a result, many classes of IoT device are more vulnerable to being accessed by malicious actors. A good example is the case of mobile-connected traffic lights in South Africa, where thieves broke into the connectivity units and stole SIM cards which were used in other devices.

5. Constrained devices

One of the key IoT trends of the last decade, well documented by Transforma Insights, is the emergence of the 'Thin IoT stack', which describes an emerging norm within the development of IoT applications to make use of specific off-the-shelf technologies that have been created explicitly to be optimised for use in constrained environments, the constraints being some combination of limited access to power, low bandwidth connectivity, and limited processing and memory.

One result of using these constrained technologies is that they often have limited capability to support security features. In some cases on-device processing is very limited, or networking protocols may not support the appropriate level of security, or the available data transmission may be so limited (due to the available technology or the desire to maintain battery life) that firmware updates are difficult to achieve. With the constantly evolving threat landscape it's critical to be able to do firmware over the air (FOTA) updates, which may not be possible with some constrained technologies.

6. Interconnectedness

An under-considered aspect of IoT security is the extent to which different systems make use of common infrastructure, opening the up to security vulnerabilities. The most common are man-in-the-middle attacks on users' Wi-Fi networks. These open up the risk of financial fraud and other serious issues. In one case, Pen Test Partners easily hacked an iKettle, to reveal the Wi-Fi password for the network on which it resided. The most famous example of this is probably the Las Vegas casino where financial details of customers were accessed by the hacking of a fish tank monitor. Target had a similar experience in 2013 when hackers made use of vulnerabilities in its HVAC system to access credit card information. And the famous Jeep hack of 2015 saw white hat hackers exploit a vulnerability in the infotainment system to get access to the CANBUS, allowing them to steer and stop the car.

7. Complexity

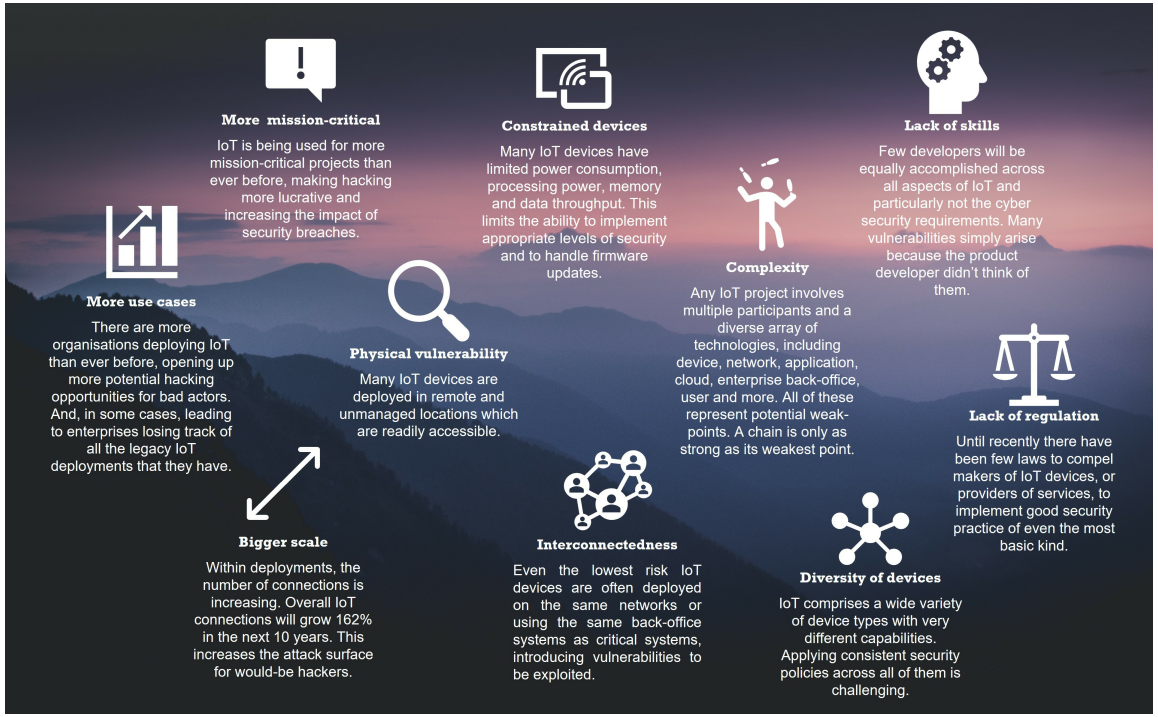
Any IoT project involves multiple participants and a diverse array of technologies, including device, network, application, cloud, enterprise back-office, end user and more. All of these represent potential weak-points. A chain is only as strong as its weakest point.

8. Diversity of devices

Managing security on IoT devices is an order of magnitude more complex than managing it for a limited array of traditional ICT devices, such as handsets, PCs and IT infrastructure. While handling device management in a bring-your-own-device environment was slightly challenging due to the variety of device types, with IoT that is expanded ten-fold. Enterprises need to consider security vulnerabilities of a diverse range of devices across generic IoT deployments, such as building automation or security, and specialist vertical use cases, such as process automation, payment terminals, track & trace or inventory management.

9. Lack of skills

There is a shortage of skills for developers in ICT in general and this is particularly pronounced in the IoT, where the set of capabilities required is very broad, spanning both hardware and software. Many security problems arise simply because the developer was not cognisant of the risks across associated domains with which they may not be too familiar.



10. Lack of regulation

This item could have been called 'manufacturer corner-cutting' because that's largely what stimulates the need for regulation. Hardware developers trying to produce as cheap a product as possible will often cut corners, and security is one of those corners. The Mirai botnet, for instance, which infected as many as 400,000 consumer IoT devices, particularly video cameras, was able to do so simply because of a lack of basic security on those devices. Regulation is needed to ensure they do not do that.

IoT security legislation

One of the key aspects of IoT is regulation. Over the last couple of years there have been some quite significant laws introduced in the US, EU and elsewhere covering IoT and particularly IoT security. It's critical to keep on top of the changes. The focus of regulation until very recently has been on providing voluntary guidelines for device manufacturers, but the coverage is expanding and the guidelines are evolving into concrete obligations in many cases. These are mostly consumer-oriented and not immediately applicable to B2B IoT, but they will become established best practice for any IoT deployment. Enterprises can and should be looking for vendors that are compliant with the salient parts of these regulations.

US

The IoT Cybersecurity Improvement Act, 2020 is focused on federal procurement of IoT but not private sector or consumers; although the aspiration is that federal procurement volumes will trigger changing behaviour by manufacturers more generally. It gives the National Institute of Standards and Technology (NIST) oversight of IoT cybersecurity risks, requiring it to set up guidelines and standards, including over reporting on security issues. NIST has a set of voluntary guidelines for manufacturers, which are promoted as capabilities consumers should look for, including a unique identifier and the ability to configure and update firmware.

On the 1st January 2020 California's Consumer Privacy Act came into force, regulating privacy requirements for Internet of Things (IoT) devices. It applies to any company that counts California residents amongst its customers. As a result, it is effectively a national (and arguably an international) law. Oregon introduced almost identical legislation on the 1st January 2020. The law covers any device that is assigned an IP or Bluetooth address and is capable of connecting directly or indirectly to the internet. Because it covers any device regardless of whether owned by an individual or a business, the law includes both consumer and non-consumer devices. The law is somewhat light on specifics, requiring ostensibly that an IoT device carries a 'reasonable' level of security that is 'appropriate' to the characteristics of the device and the information that it collects, stores or transmits. There are a few mandated requirements for devices connected via wide area networks. Each device must have either a unique pre-programmed password or must contain a security feature requiring the user to generate a new means of authentication before getting access to the device for the first time (i.e. the user be required to set a password).

EU

The EU Cybersecurity Act which came into force in 2020 placed a requirement on ENISA, the European Union Agency for Cybersecurity, to define a certification framework for ICT products and services, which was released in November 2019 as "Good Practices for Security for IoT – Secure Software Development Lifecycle". This focused on ensuring security is baked in to the software development lifecycle for IoT. However, it contains only 'good practices and guidelines' rather than regulations. This voluntary certification scheme will be reviewed periodically.

The EU Cyber Resilience Act was published in September 2022. It will address the current low level of cybersecurity within IoT devices and the need for software and firmware updates to patch vulnerabilities. Features will include minimum password standards, the ability to support software updates, some form of vulnerability testing and restrictions over the use of personal data. It will apply to manufacturers and developers across hardware and software and include substantial fines for non-compliance. It is likely to include requirements for providing buyers with greater product information as well as prohibiting the sale of devices that do not comply with requirements. After adoption by the EU there will be an implementation period by national governments, meaning that the obligations are likely to apply from some time in 2025. National governments are also able to apply their own national rules independent of those of the EU.

Other relevant regulations include the NIS2 Directive, introduced in January 2023, which is focused on encouraging member states to harmonise cybersecurity rules, examine current vulnerabilities, establish national cybersecurity strategies, and the wider General Data Protection Regulation (GDPR) which covers the use of personally identifiable data.

The European Telecommunications Standards Institute (ETSI) is a standards body rather than an arm of government and as such does not have legislative power. However, its Consumer IoT Security standard EN 303 645, released in June 2020, has 13 recommendations including no default passwords, a requirement for software updates and inclusion of features to allow users to delete personal data.

UK

At the start of 2020, the UK set out a Code of Practice for Consumer IoT Security, representing a progression from the initial voluntary approach. It focuses on consumer devices only, although there is reference to extending it to enterprise in due course. It is slightly more explicit than that seen in the US, with thirteen guidelines from the ETSI 303 645 standard, and three main requirements:

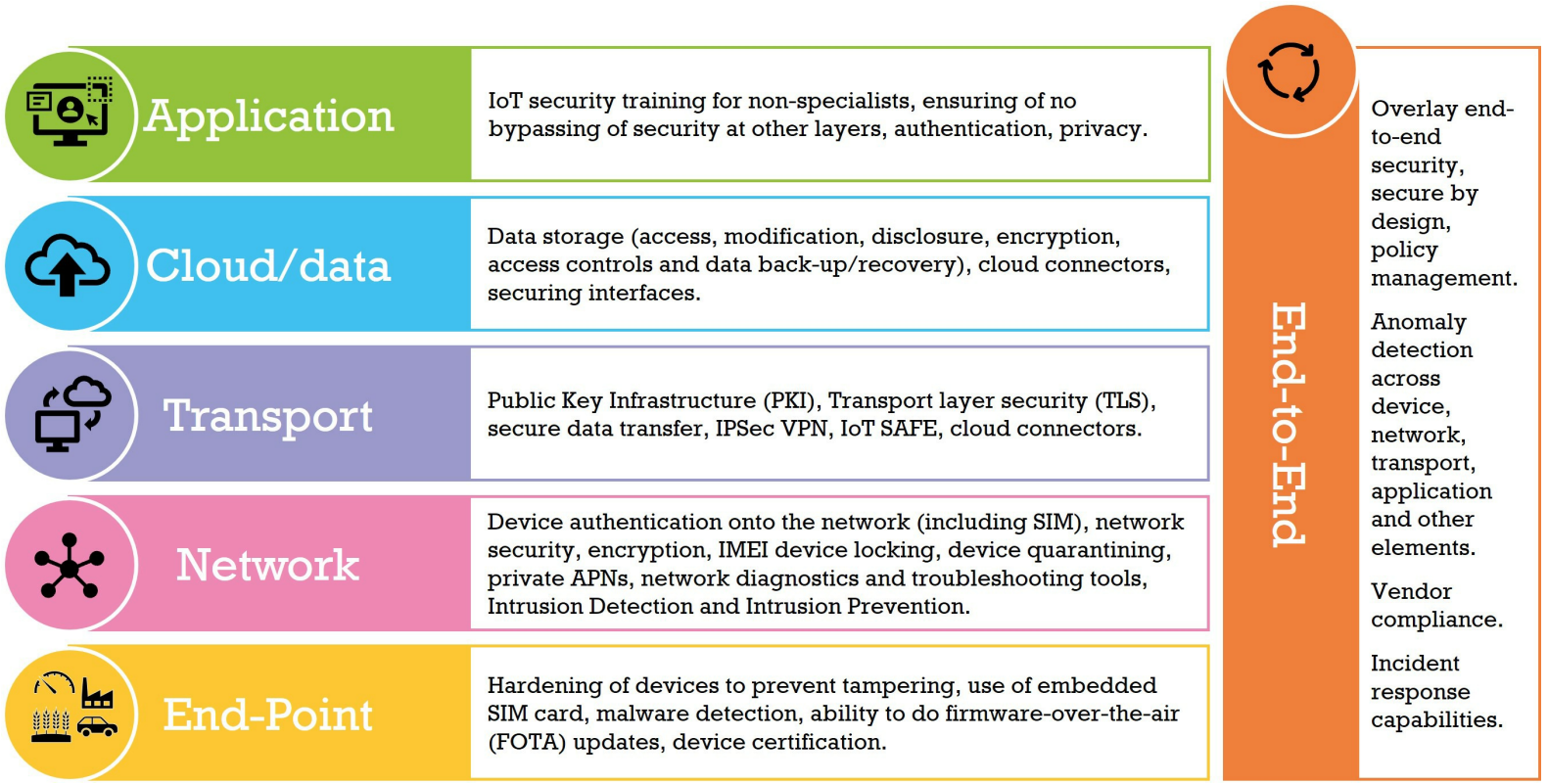
- IoT device passwords must be unique and not resettable to universal factory setting.
- Manufacturers must provide a public contact point as part of its vulnerability disclosure policy.
- Manufacturers must explicitly state the minimum length of time during which the device will receive security updates.

This is set to be superseded by the forthcoming Product Security and Telecommunications Infrastructure (PSTI) Bill, which places requirements on manufacturers and vendors of IoT devices to meet new cybersecurity standards. This includes provisions such as a requirement for transparency over features and functionality, better public reporting system for vulnerabilities, and a ban universal default passwords.

IoT security layers

The six layers of IoT security

[Source: Transforma Insights, 2023]



TRANSFORMA INSIGHTS

IoT security layers

What do we mean when we talk about 'IoT security'? IoT deployments are relatively complex, comprising devices, networks, platforms, applications, enterprise back-office systems on so forth. We identify six main security layers.

End point

The first consideration in IoT security is likely to be the 'thing'. The top priority within devices will be hardening to prevent tampering. This applies both to the overall device itself, and to the specific case of the SIM card. The latest generation of embedded SIM, or eSIM, is soldered into the device to prevent its removal.

Within the end point/device category we also include having the capability to do FOTA updates. This necessitates having the appropriate network technologies to handle the required data throughput (many LPWA technologies will not be able to handle it), as well as the required storage and processing on the device.

From a device firmware security standpoint, at the device layer the main priority will be malware detection.

Network

Network security is generally very good, particularly on mobile networks. But that is not to say that there aren't also vulnerabilities here. This is exacerbated for IoT applications that are supported over a number of networks and peering points, including the public internet.

Vulnerabilities, even in mobile networks, have been exploited, for instance by pinging the HLR/HSS to identify a device's location, or by enacting denial of service attacks via the HLR/HSS.

Network security incorporates device authentication (including SIM authentication) and network encryption. We include here functions such as private APNs, network diagnostics and troubleshooting, IMEI device locking (i.e. preventing a device from connecting to any other network), quarantining of devices, and DNS white-listing. Also anomaly detection might be done at the network layer too. In some cases, IoT connectivity providers deploy specific Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Transport

In many cases, enterprises deploying IoT will consider that network layer security alone is not sufficient. And furthermore, many cloud providers demand some Transport Layer Security (TLS) for data delivery into the cloud. Typical approaches to TLS use a hardware security module (HSM) or cloud providers' SDK on the device.

Features relevant here include the provision of IPsec VPNs, and varying approaches to managing a private global backbone, including cloud-to-cloud peering. Ideally IoT traffic should not be sent via the public internet.

At the Transport layer, the most interesting latest development is IoT SAFE (the IoT SIM Applet For secure End-to-end communication), developed by the GSM Association to allow for the use of the SIM card as a standardised hardware 'Root of Trust' for managing authentication between IoT devices and, typically, cloud servers. It provides mutual authentication between the end points and applies Transport Layer Security (TLS) to the end-to-end communications.

Cloud/data

This section applies equally whether the data is stored in the cloud or on-premises. Data storage considerations include protection from unauthorised access, modification or disclosure, the application of encryption, access controls and data back-up/recovery plans. As noted above, many cloud providers have specific requirements for security, in terms of protocols to be used for data transport. Other aspects of cloud security relevant for IoT include credentials, provisioning, access control, and device SDKs. Many cloud providers have a set of robust security-related tools for anomaly detection. Other issues for consideration at this layer include lack of security in interfaces and APIs, and data breaches.

Application

Many security vulnerabilities derive from how applications are built. Often considerations for security will be low on the list of priorities. The key is to ensure that application developers are aware of security requirements and build the application in a way consistent with the security capabilities at lower layers. The application itself will handle authentication of users and data privacy.

End-to-End

The concept of 'End-to-End Security' includes four main elements. First how the IoT application is built, considering all the security elements as a whole, e.g. using 'secure by design' principles, or having a consistent approach to update management. The second is to incorporate and integrate information from all layers to provide optimised security. The includes things like anomaly detection across device, network and transport layers. The third relates to ensuring that all the third party vendors have compliant security measures. The fourth is to have appropriate incident response capabilities, establishing procedures for identifying, containing, and removing cyber threats, and communicating with stakeholders, including law enforcement.

Framework and functions

As discussed in the sections above, there are growing security threats in IoT. Enterprises must be thinking both strategically about the best framework to establish in order to address security, and at the same time have one eye on the specific tools to be used.

Framework

An IoT Security framework should cover the following:

- **Dimension the problem.** Enterprises need an audit of devices, vulnerability assessment, penetration testing, and cyber attack simulations, to understand the security challenges and to have a rigorous approach to addressing them.
- **Understand your capacity for risk.** The appropriate level of security will always be dictated by a company's circumstances and its willingness to trade-off other factors (e.g. price or ease-of-use) in order to increase security. There is such a thing as too much security.
- **Secure end-to-end.** The Internet of Things comprises a lot of different domains, any of which could be the weak point.
- **Secure by design.** End-to-end security should be considered during the process of developing the IoT solution, not overlaid at the end.
- **Establish policy and processes.** This might include things like network separation, strong passwords, use of public key infrastructure, and certificate management. It might also include compliance with standards, and consideration of ransomware insurance.
- **Compliance.** Establish a mechanism for ensuring that you are compliant with the ever-changing regulations relating to IoT and particularly security.
- **Train your people and partners.** The biggest security risk is generally the failure to follow established practices, which can be mitigated by training, including business certification such as ISO and Cyber Essentials.
- **Manage your partners.** You will almost invariably rely on third-parties for the provision of parts of your IoT project. You must also be confident that they are complying with best practice for security. Do your due diligence on them and their security practices.

Functions

In parallel with the framework strategic considerations are the specifics of the IoT security features which should be implemented. The below are some of the most obvious mechanisms for mitigating security risks and should almost invariably feature as part of the considerations for securing an IoT deployment:

- Harden your devices to remove the risk of physical security breaches.
- Ensure that your devices can handle the necessary FOTA updates.
- Use features such as private APNs, IoT SAFE, and IPsec VPNs for robust network and transport layer security.
- Ensure continuous management of authentication and authorisation, for instance using hardware root of trust and digital certificates.
- Implement anomaly detection across all aspects of the IoT deployment, incorporating device, network and cloud.
- Apply automatic responses to security threats, for instance quarantining devices by blocking or constraining them.
- Remediation. And it needs to deal with breaches when they inevitably do happen.

Across these two areas of Framework and Functions there is a common aim: minimising the risk from IoT security risks, through establishing robust mechanisms for mitigate risk, reacting to breaches, and remediating.

IoT Security-as-a-Service

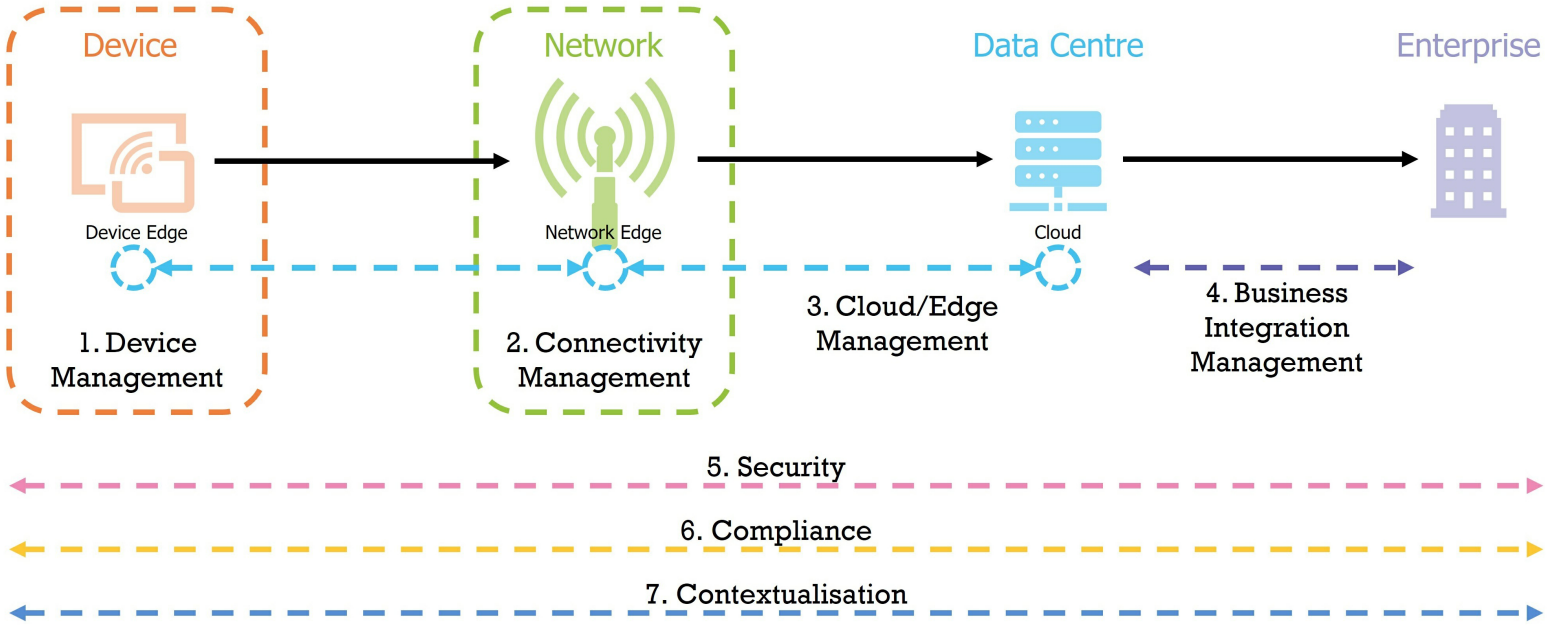
The complexity of building IoT solutions and the general lack of skills amongst most enterprises to span the entirety of the diverse elements of an IoT solution, mean that it is inevitable that IoT will be delivered predominantly as a managed service, rather than a stand-alone platform or product. Enterprises deploying IoT need trusted partners for the various elements. As part of its ongoing research on the evolving IoT landscape, Transforma Insights has identified a set of seven 'Service Domains' that will define how IoT is delivered . One of these domains is Security.

As outlined in the sections above, IoT security is a multifaceted and constantly evolving technology area. Few enterprises can be completely confident in their ability to stay on top of all of the constituent parts across end-point, network and transport security, cloud/data security, solution design, anomaly detection, policy management, incident response and the other areas noted above.

The solution is to look for partners (and it's unlikely that a single partner will necessarily be able to cover every aspect) that can provide the IoT Security-as-a-Service function that will help to minimise an enterprise's risks.

The 7 Service Domains of IoT

[Source: Transforma Insights, 2023]



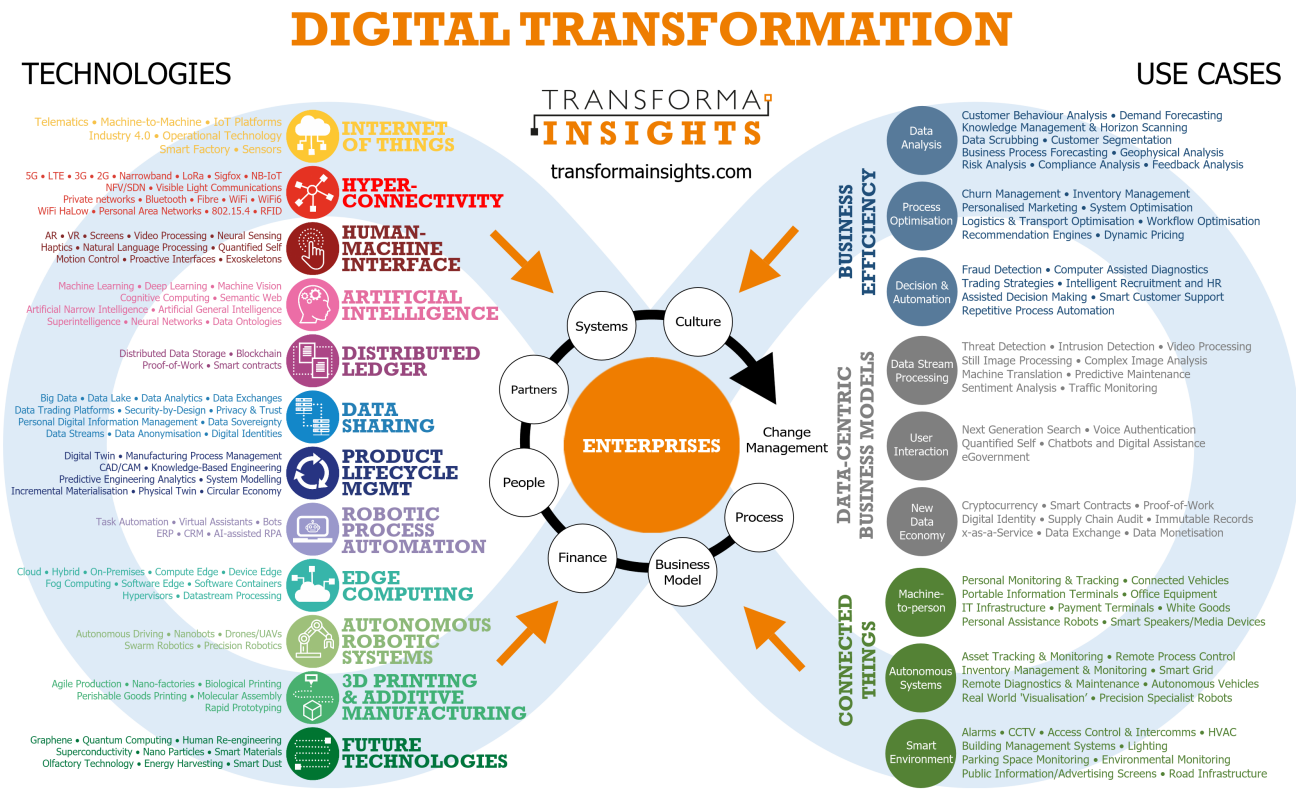
TRANSFORMA INSIGHTS

About Transforma Insights

Transforma Insights is a technology industry analyst firm focused on the impact of emerging technologies and the associated technical and commercial best practice.

We help technology adopters understand the opportunities associated with new technologies, particularly the Internet of Things, but also in Artificial Intelligence, Distributed Ledger, Edge Computing and others under the umbrella of 'Digital Transformation'.

We help technology vendors understand the changing market dynamics and the associated market opportunity.



transformainsights.com

enquiries@transformainsights.com

@TransformaTweet

TRANSFORMA INSIGHTS