IoT Now: ISSN 2397-2793

IoTNOW

HOW TO RUN AN IoT ENABLED BUSINESS

The IoT Now Guide to IoT Security 2022

INTERVIEW

Thales' Stephane Quetglas explains how IoT can be secured end-to-end at scale

THALES
Building a future we can all trust

Improving IoT cyber security

through eSIM-based scalable trust

The IoT Now Guide to IoT Security 2022

IN THIS ISSUE

4 COMMENT
George Malim chalks up another skirmish in the eternal battle of good versus evil

5 SECURITY NEWS
Critical infrastructure operators increase cybersecurity spending, healthcare sector security concerns remain, enterprises to spend US$227bn on cybersecurity in 2027

6 INTERVIEW
Thales' Stephane Quetglas tells George Malim how IoT can be secured at scale thanks to new methods for securing IoT devices

10 IoT SECURITY REPORT
Our six-page report reveals how OEMs and IoT solutions providers can address the challenges of achieving security by design through harnessing new technologies such as eSIM and iSIM and initiatives such as GSMA's IoT SAFE

16 SECURITY BY DESIGN
Bob Emmerson takes a tour through the latest security concepts enabling improved security for IoT devices

IoT security steps up for the mass-market with SIM innovations

From fish tanks to traffic lights, connected devices present back doors through which cybercriminals can attack. We've become familiar with tales of esoteric devices being hacked and then used to defraud, damage or deter organisations' digital operations. For IoT insiders, on the eve of the mass market's arrival, the future looks terrifying but improved security options are arriving just in time, writes George Malim

The casino fish tank used as an entry point by cybercriminals is a well-worn tale that sits alongside surveillance camera footage being hacked and used in ransom attempts in the often-repeated warnings about IoT. These examples provide just a hint of the threat surface of IoT in which everything from smart manufacturing robots to basic connected things such as pet or child trackers could be used with malicious intent by bad actors.

The IoT industry and the IT industry have been engaged in a continuous battle with criminals as they attempt to secure networks, devices and other hardware but the situation is a war of attrition. No sooner has a security innovation been brought to market than the criminals come up with ways to circumvent it or, if the measure is truly successful, they move on to target other weaknesses. One vulnerability facing IoT devices has been the plastic SIM card. Itself a highly secure element, the SIM card assures the identity of the mobile service subscriber enabling secure billing and the tying of the connection to a customer or user. However, it all falls apart if the SIM card is removed, as happened in the early days of IoT when criminals removed SIM cards from traffic lights in South Africa and slotted them into their phones to make calls.

The SIM is great if it stays in place and embedded and integrated SIMs (eSIM and iSIM) are moving SIM security on another step. With the SIM permanently soldered to the device, there is no simple means for it to be removed easily and a SIM that is part of the payload of the module similarly cannot be changed physically. This makes the SIM a tamper-resistant secure element within an IoT device that is far harder to alter, hack or damage than a plastic SIM card. In addition, it offers compelling advantages of tightly tying the user identity to the device rather than just the connection.

George Malim, managing editor

Administered within GSMA's IoT SAFE initiative, the SIM becomes more than an identifier, it becomes an enabler of trust with all the associated business benefits that brings. This creates a root of trust that can be fundamental to embedding security by design within IoT devices.

Does that mean we can all relax when it comes to IoT security? Certainly not, but it does mean the good guys have won this round of the eternal security battle.

Enjoy the Guide!

George Malim

MANAGING EDITOR
George Malim
Tel: +44 (0)7930 301 841
g.malim@wkm-global.com

EDITORIAL DIRECTOR & PUBLISHER
Jeremy Cowan
Tel: +44 (0) 1420 588638
j.cowan@wkm-global.com

DIGITAL SERVICES DIRECTOR
Nathalie Millar
Tel: +44 (0) 1732 808690
n.millar@wkm-global.com

SALES CONSULTANT
Cherisse Jameson
Tel: +44 (0) 1732 807410
c.jameson@wkm-global.com

DESIGN
Jason Appleby
Ark Design
Tel: +44 (0) 1787 881623

PUBLISHED BY
WeKnow Media Ltd. Suite 138,
80 Churchill Square, Kings Hill,
West Malling, Kent ME19 4YU, UK
Tel: +44 (0) 1732 807410

Critical infrastructure sectors ramp up cybersecurity spending

Global cybersecurity spending in industrial critical infrastructure sectors such as energy, transport and water and waste management, is expected to hit US$23 billion by the end of 2022 and grow at a CAGR of 10% to reach US$36.67bn in 2027, according to a new whitepaper from **ABI Research**.

"Businesses, industries and in fact the entire world, have never been more connected than they are right now. They have also never been more at risk," said Michela Menting, the Digital Security research director at the firm. "Organisations and verticals continue to integrate technologies like the Internet of Things (IoT), 5G and blockchain, meaning more points of connection - and points of vulnerability - than ever before. As a result, ensuring security is not just a hardware issue or a software issue - it is a web of challenges and solutions spanning entire technology ecosystems."

Among the trends highlighted in the whitepaper, ABI Research cites adoption of IoT cybersecurity as essential for optimising data security in telematics in order to enable intelligence-driven monetisation. The paper says secure data management for automotive telematics is becoming increasingly important for vehicle manufacturers, tier one suppliers, telcos and insurance companies. Almost every aspect of the software-defined vehicle is set to include constantly evolving cybersecurity technologies at the hardware, software and network level, with telematics data security being one of the core operations.

In addition, distributed working environments and increased remote working are affecting both workers and assets in IT, OT and IoT. Secure connectivity and identity management have become key priorities in disparate and heterogenous networks as a result and all these elements are driving demand for hardware security.

Michela Menting, ABI Research

Digitisation of healthcare speeds up but security concerns remain

As the pandemic disrupted traditional patient service models, the healthcare sector overwhelmingly adopted remote and telehealth technology solutions. Research from **SOTI**, has reported that nearly all global healthcare providers (98%) offering frontline services have implemented IoT/telehealth medical device capabilities.

The increased adoption of new technologies in the healthcare sector is evident in 73% of IT healthcare professionals indicating they have increased their annual technology spend since 2020. The rise in healthcare IT investments appears to be focused on three key elements: interconnectivity, automation and data management. Research revealed that 75% of IT healthcare professionals agree patient services benefit from heightened interconnectivity, 72% agree the use of artificial intelligence (AI) in patient care enables medical staff to treat more patients and 94% stated digital patient recordkeeping increases efficiency and enhances data sharing.

As part of its report, SOTI surveyed 1,300 healthcare IT professionals across the US, Canada, Mexico, UK, Germany, Sweden, France and Australia to understand how their organisations pivoted to provide patient care throughout the pandemic, the role technology played in delivering positive patient outcomes and what major obstacles remain.

"Following the COVID-19 pandemic, mobile and IoT devices have become vital for healthcare organisations, allowing them to quickly adapt to changing circumstances, alter patient care methods and improve health outcomes," said Stefan Spendrup, the vice president of sales for Northern and Western Europe at SOTI. "Almost all UK healthcare providers (97%) offering frontline services have now invested in IoT/telehealth medical device capabilities."

Regarding data security, 86% of IT healthcare professionals are worried about patient information being revealed, lost, accessed, stolen or inadequately backed up. These are justified concerns as 70% of organisations have experienced a data breach since 2020. In addition, 57% of IT professionals believe patient data security is more at risk than ever, while 46% agree their organisation does not spend enough money on data security.

Stefan Spendrup, SOTI

News in Brief

Enterprise cybersecurity spend to exceed US$226bn globally by 2027

A new study from **Juniper Research** has found the value of enterprise cybersecurity spending will exceed US$226bn in 2027; up from US$179bn in 2022. This growth of 26% over the next five years reflects the increasing maturity of the cybersecurity market, which continues to evolve as new threats emerge. The report identified a rising awareness of vulnerabilities, alongside emerging threats, including ransomware and distributed denial of service (DDoS) attacks as key drivers behind the increasing spend.

"Cloud computing has been transformative for businesses, so it is no surprise that two of the biggest cloud computing vendors, **AWS** and **IBM**, also lead in the cybersecurity space," said research co-author Damla Sat. "For cloud vendors, effective cybersecurity is a basic requirement by offering in house cybersecurity solutions, AWS and IBM are capitalising on their existing large user bases; acquiring businesses and capabilities as needed to enhance their product offerings."

How IoT SAFE improves IoT cybersecurity whilst being simple to deploy at scale

Security in IoT has often been listed as a development priority but then postponed or neglected with negative consequences. As the attack surface expands and new threats proliferate, traditional approaches to securing devices are too inflexible, too expensive or too complex to integrate to meet the timescale and volume needs of IoT enterprises. Current security methods address security concerns but are fragmented and this prevents them from being able to scale up. In the field of cellular connectivity, the GSMA's IoT SAFE initiative provides an alternative for IoT enterprises that is independent of mobile operators and provides a standardised method for securing IoT devices. This, Stephane Quetglas, the director of marketing for embedded products at Thales, tells George Malim means IoT can be secured end-to-end at scale, with flexibility to change connectivity provider and without the need to re-invent the wheel for every device or service ▶

SPONSORED INTERVIEW

Stephane Quetglas
IoT Marketing Director
Thales

We've seen the attacks on IoT devices and services for more than ten years and IoT security remains a significant concern for us

George Malim: What are the challenges of addressing the sheer volume of IoT attacks?

Stephane Quetglas: We've seen the attacks on IoT devices and services for more than ten years and IoT security remains a significant concern for us. There have been some substantial disruptions caused by security and the situation has not improved much over the years because there are more and more companies wanting to connect their devices and to deliver more value and have more mobile services. Companies have started to put functionality and the service itself at the top of their list and not the security. This is because they haven't been sufficiently aware of the security issues that exist and the additional security issues that exist when you connect a device to a network.

The scale of IoT is enormous and is well beyond the availability of skilled security experts in the industry so companies tend to forget about security or use very simple methods such as log-in passwords. When you use passwords and don't pay attention to them, you risk having a password that is too simple or shared across devices, making all of them vulnerable at once.

The main barriers come down to shortage of security skills and the cost of implementing security in IoT. Implementing security has a cost and whatever the device it is important to diversify the secure credentials that you deploy in the device. This is so that if a device is attacked, other devices are not vulnerable to risk, but this process is costly.

The other big reason that implementing security in the proper manner is very costly is the need for solutions that address both the level of security required and the level of scalability needed. This is in the context of billions of IoT devices so the scale is huge and will be even larger in the context of the new generation of 5G and low power networks which are arriving and bringing an even greater number of connected devices.

In addition, there are use cases where there's a need for securing the connectivity of the device to the IoT application and this relates to the value of data. Apps increasingly are deployed in the cloud and that means you need secure connections so you can sign data when you send it back and it can be verified. For example, in use cases in the energy, automotive or healthcare industries the value lies in the type of data that is exchanged, not in the fact that the platform is cloud-based..

In addition to public networks, in private networks you have use cases where the data circulating needs to be certified so it can be trusted. IoT in private networks such as at manufacturing sites relies on the ability for devices to sign data and prove it is genuine. There are more and more use cases emerging that require security in this way so scalability is essential.

GM: How does the GSMA's IoT SAFE initiative solve the issues by making use of the hardware's tamper-resistant element?

SQ: The tamper-resistant element is the subscriber identification module (SIM) or embedded SIM (eSIM) already in use in connected cars, smart meters or container trackers. That's the first element so the obvious choice is to build on what is already in the connected device. It is the first step to address scalability requirements because you don't have to add another chip or element to your bill ▶

Security by design is for us at the heart of what we do but lack of skills and the complexity of security means companies in IoT are not comfortable with it

of materials (BOM). The SIM and eSIM offer a very high level of security and have been used for many years so they are a perfect platform for a security solution.

The second choice is to adopt an approach based on public key infrastructure (PKI) which provides a cryptographic method used for strong authentication between cloud and devices and data integrity. Typically, you might use this method on your computer to access online banking. The PKI technology allows you distribute strong credentials in a secure and scalable manner unlike a login/password.

The two main choices therefore come down to re-use of the field-proven tamper resistant element that is the foundation of SIM and eSIM, with a PKI approach, which is very appropriate for addressing the security issues IoT faces. When done in a standardised manner like IoT SAFE, this is ideally suited to scale and manage large volumes of connected objects.

GM: What is your view of security by design and is this approach being taken by the IoT industry?

SQ: It is very important and needs to be considered as an essential part of device or service design. Security by design means that you consider security at the earliest stages of your process when you first think about creating an offering or business. If you do this, you will have the right foundations.

Security by design is for us at the heart of what we do but lack of skills and the complexity of security means companies in IoT are not comfortable with it. This is counter-productive because it is very difficult to fix security issues when products are already in the field and you face issues that you cannot repair or address.

Security is increasingly put as a high priority by IoT companies, and they are interested in relying on security specialists to try and bring the right approach. This is partly to do with the skills shortage but also because security is evolving all the time. To be effective, you need to know the security ecosystems, learn skills and understand new attacks and ways to counter them.

This continuous process is difficult to implement, especially for small-to-medium enterprises. Don't forget IoT is made up of lots of small companies, it's not just a few big names so for many it's very difficult to develop in-depth security skills.

GM: How are the IoT SAFE specifications being integrated into hardware tamper resistant elements?

SQ: What is key for IoT SAFE is that this is a standardised approach that utilises the eSIM independently from the mobile network operator. If you use IoT SAFE in the eSIM in your connected devices, you can choose a network operator to provide connectivity and use IoT SAFE to connect devices to your IoT cloud and later on, if you want, you can change the mobile operator for your connectivity without impacting your IoT service.

Indeed, devices will still be able to connect to the same cloud with the same credentials even after the mobile operator has been changed. IoT SAFE is not included in the mobile network operator profile, but in a dedicated security domain sitting beside the SIM application on the same tamper-resistant element. The flexibility this provides is important for IoT enterprises because IoT SAFE can be independent across the connectivity provider and the security provider.

The freedom this provides means there are fewer constraints in terms of vendor selection and the security can scale which is not the case when you have fragmented systems.▶

We work with providers of security stacks and middleware vendors to make sure IoT SAFE is already supported and thus the integration made easy for device makers

GM: What is Thales' approach to IoT SAFE and how does that deliver scalable trust for IoT applications?

SQ: We embraced IoT SAFE immediately. We are convinced of the need for improved IoT cybersecurity and the requirement to provide a security solution to IoT players that provides something standard and therefore scalable. Standardisation is the right way to go so the security solution can be deployed everywhere.

IoT SAFE is standard but of course you have some additional value as a vendor that you can provide to your customers. We work with providers of security stacks and middleware vendors to make sure IoT SAFE is already supported and thus the integration made easy for device makers. We also provide a touchless provisioning service which is a way to totally remove the cost impact of adding security into a device when the device is manufactured. When you use Thales' IoT SAFE in the device, there is not additional activity and no additional charge in the process because our solution will automatically generate and validate credentials when the device is first used on the field.

This is how we provide additional value. Of course, we have connectivity management solutions and we're a leader in eSIM and remote SIM provisioning (RSP) solutions and this means we are able to provide our customers with complete solutions for connectivity and security.

GM: What are the alternatives to IoT SAFE?

SQ: The most popular alternative is a device-based approach where security is implemented as software in the device memory. This solution works from a functionality perspective but is quite bad from a secure path point of view because a general purpose processor in the device is not protected and is very easy to defeat. In addition, device-based solutions are usually proprietary or bespoke to a specific device so you need to repeat the same work for every device or implementation and this approach can't scale.

Another alternative is Generic Bootstrapping Architecture (GBA) which is a user authentication method based on the SIM application. This is mobile operator-centric and was standardised a long time ago. Adopting this method means you require a security service provided by your mobile operator: as a consequence, you lose the service if you change operator and need to integrate with the security service of the new operator. In addition, this does not provide true end-to-end security up to your cloud platform.

IoT SAFE can be deployed in the same way across all of your devices and it is not linked to your mobile operator. The security provided is end-to-end so you are truly protected.

GM: Are IoT enterprises adopting IoT SAFE?

SQ: We are seeing strong interest in IoT SAFE today and people that are using cellular technology for IoT are highly accepting of this solution because secure network connections and data are very important to their business cases. Having said that, awareness needs to be developed further to detail the potential of the technology. We're working to make sure IoT players are aware they can use and rely on it to relieve some of their pain points and ensure their IoT operations are secure.

Sponsored by:

THALES
Building a future we can all trust

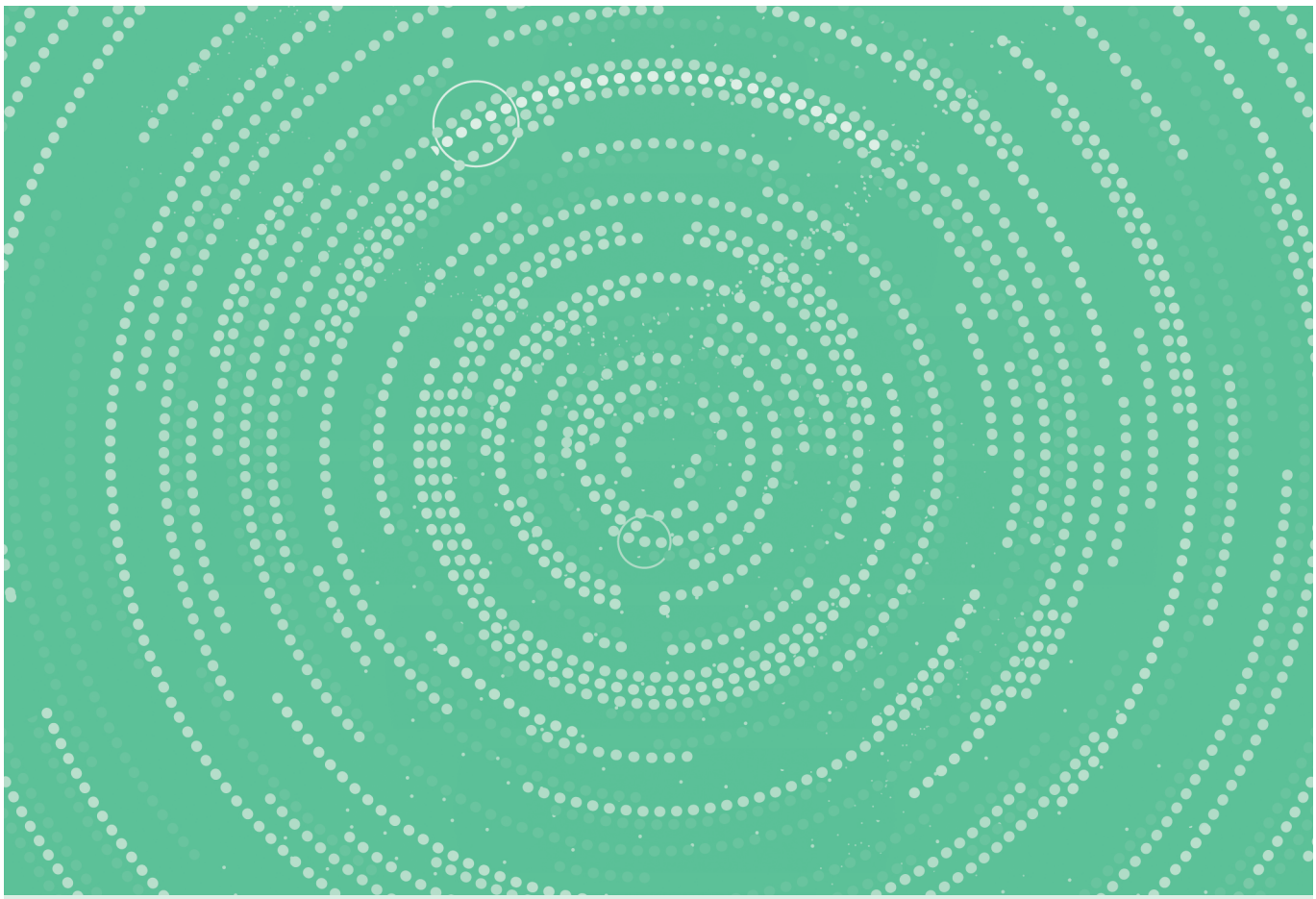
How OEMs and IoT solutions providers can address the challenges of achieving security by design

As IoT continues to mature and the volumes of connected IoT devices increase, the attention has turned to securing IoT. The larger number of devices have resulted in an expanded threat surface and greater opportunities for cybercrime. For OEMs and IoT solutions providers this presents two fundamental challenges: reducing crime and strengthening trust in IoT devices and the data they transmit

Analyst firm **Gartner** reports that more than 80% of organisations have implemented some form of IoT and close to 20% have detected an IoT-based attack in the past three years. This demonstrates an ever-growing number of IoT enterprises feeling the negative effects of security breaches but there is still significant failure to put adequate IoT cyber security in place. The firm says fewer than one-third of chief information security officers are confident their information security can reliably assess and mitigate IoT risks. This will not help breed trust and confidence in IoT devices and data among users and customers.

Reducing crime and the opportunity to commit cybercrime are obvious priorities but being able to trust IoT devices, their identities and their data is the foundation of many IoT business cases and represents the future of IoT revenues. Only when data is trusted to come from a specific device and the security of the data itself can be assured can it be relied upon and used to feed the business need it serves. Fostering trust is therefore as important as preventing frauds and cybercrime to the success of IoT initiatives. ▶

SPONSORED ANALYST REPORT



Importantly, IoT clouds are also under attack so threats are not just confined to device security. FireEye's threat intelligence and incident response unit **Mandiant** has identified a flaw in a component of the Kalay cloud platform that can be exploited to hack systems. Many Kalay users are video surveillance devices and the vulnerability has the potential to allow attackers to intercept live audio and video data. This hack relies on accessing a Kalay user's unique ID but it illustrates that IoT devices should not be seen as the only weak point and IoT cloud security will increasingly need to be addressed.

Regardless of where the attacks come, the reality is that they are increasing in frequency and systems designed to secure devices are themselves potential points of vulnerability. Cybersecurity specialist **Kaspersky** detected 1.5 billion attacks against IoT devices in the first half of 2021 via its network of honeypots which simulate a vulnerable device. This is twice as many attacks as the honeypot network recorded in the first half of 2020.

From cameras to combines, the attacks proliferate

Examples of IoT device security breaches range from surveillance cameras to combine harvesters. Last year, a group of hackers claimed to have breached a massive store of surveillance camera data collected by start-up **Verkada**. This allowed access to live feeds of 150,000 cameras inside hospitals, police departments, prisons and schools as well as at enterprises. Companies that had footage exposed included **Tesla** and **Cloudflare** and hackers said they had access to the full video archive of all Verkada customers.

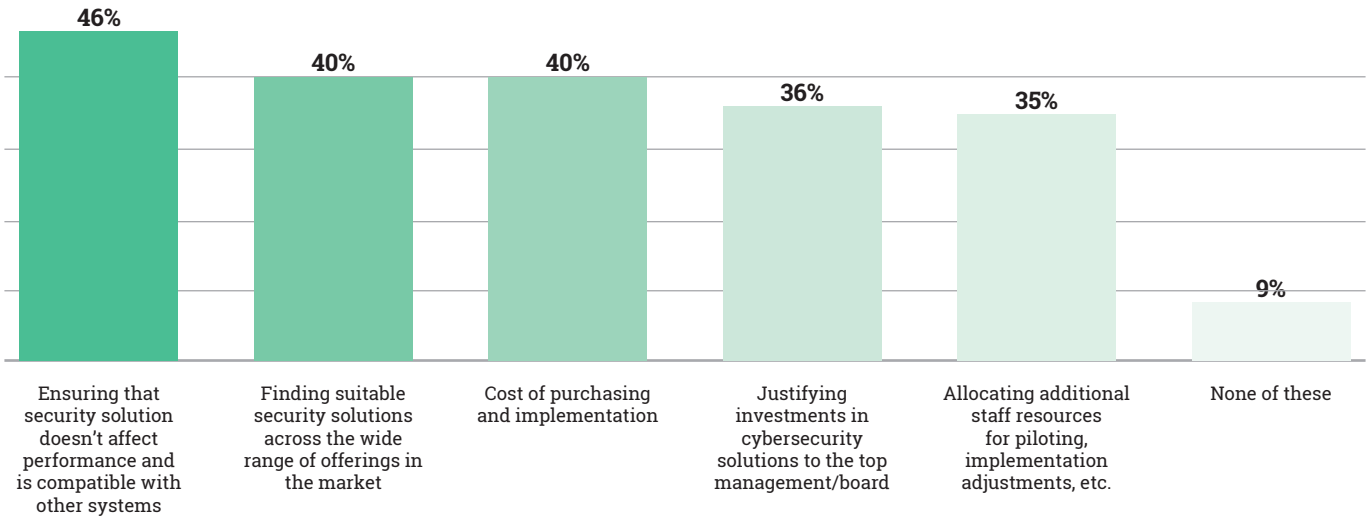
These types of examples illustrate the need for IoT service providers and original equipment manufacturers (OEMs) to adopt a security by design approach that prioritises thinking about security at the design stage and sets out what mechanisms will be used and how these will be deployed and managed when large volumes of devices are in deployment. Of course, in lower-end IoT services this needs to be accommodated at very low cost so the cost of securing the device doesn't outstrip the value of the service it provides.

Can IoT afford the cost of security?

Today there are 8.6 billion IoT connections, according to **ABI Research**. By 2026, that number will nearly triple to 23.6 billion and securing these will involve substantial investment. The firm says total revenue in the IoT security market will reach US$16.8 billion by 2026. That suggests that a typical IoT connected device could be generating revenue for security providers of 66 cents. For many types of deployment that additional cost will break the business case, while for others it will reflect tremendous value.

However, it may not be possible to extrapolate the ▶

Figure1: Top issues organisations face with cybersecurity solutions
Source: Kaspersky



numbers so simplistically. ABI Research says the amount of IoT security revenue does not always correlate with the amount of IoT connections, and some markets are expected to experience disproportional revenue as companies spend to address security.

The headline figure does illustrate a market in which there is willingness to devote sustained investment to security and that is encouraging. Even so, there's a substantial hill to climb even with this level of projected investment. In addition, not every organisation is fully-aware or committed to securing their IoT devices – yet.

Kaspersky reports that, while two thirds of organisations (64%) globally use IoT solutions, 43% don't protect them completely. This means that for some of their IoT projects, businesses don't use any protection tools. The damage to customers, the brand and its reputation cannot be allowed to continue so greater investment is needed.

For OEMs and IoT service providers there are several important concerns, which Kaspersky has highlighted in **Figure 1**. It says 46% of businesses fear that cybersecurity products can affect the performance of IoT while 40% feel it can be too hard to find a suitable solution. There are also concerns about lack of skilled staff or specific IoT security expertise within the business, with 35% citing this as a top issue.

How to improve IoT cyber security

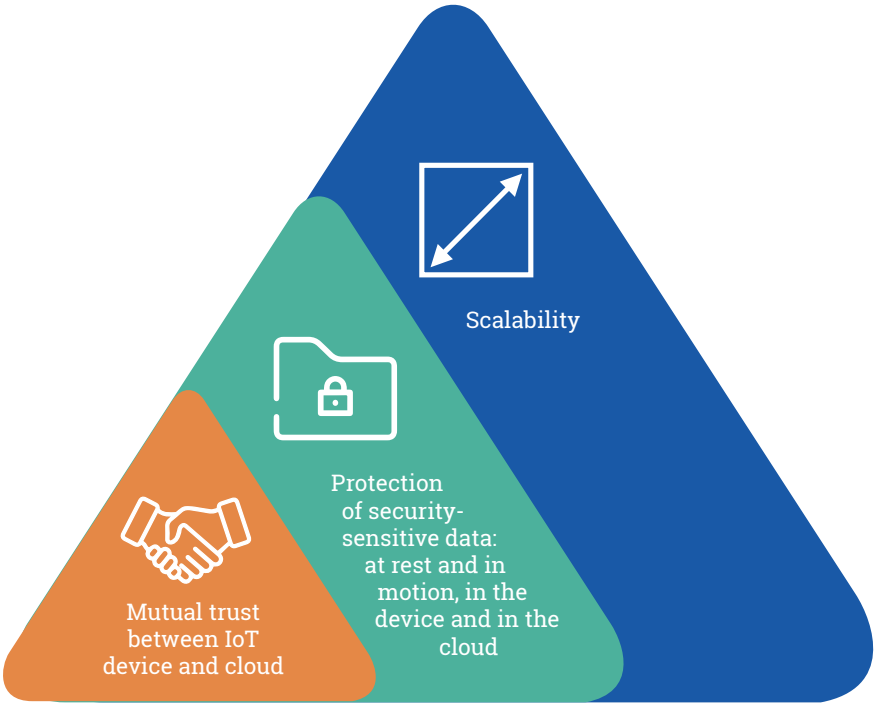
The wide array of attacks from distributed denial of service (DDoS) to malware and hacks on passwords creates a series of challenges for OEMs and IoT service providers to address on behalf of organisations that deploy IoT. In some cases, enterprises will try to address issues themselves but IoT service providers and OEMs are typically better-placed to secure IoT.

This is because they have experience of working across multiple types of devices, use cases, markets and jurisdictions so they are well aware of the correct techniques to use. They have both the IoT and security-specific skills needed, that are in short supply in the market. It will, for example, be hard for an enterprise to find the right people and the right structure to position their security stance effectively to protect their IoT operations.

The utilisation of cybersecurity is an important step but having the correct policies in place to support secure IoT is essential. Too many devices ship with default passwords or are subject users who change their password to something as simple as the word: "password."

A large proportion of security breaches can be attributed to human error so efforts made by OEMs and IoT service providers to take matters out of users' hands and embed security into IoT devices promise strong results. ▶

Figure 2: Hardware tamper-resistant elements deliver scalable trust for IoT applications.
Source: Thales



The alternative is for enterprises to do it all themselves and invest in cybersecurity software, vulnerability management tools, password management software, network intrusion detection systems and so on. Each of these must be kept up-to-date, managed and maintained and adds a significant non-core list of tasks for an enterprise.

What can OEMs and IoT service providers do?

In addition to bringing their experience to customers they can assist by setting out how security by design can be achieved. Security by design is an approach to software and hardware development that moves security from being a bolted-on afterthought to a primary consideration undertaken at the design stage of an IoT device or service. Security by design will always outperform retrospective measures to addressing existing vulnerabilities and patches and is becoming essential in IoT as connected devices are readily addressable over the internet.

OEMs and IoT service providers can use their knowledge to assist customers to design security into their devices and ensure manufacturing itself is secure so authentication, for example, is protected. Other innovations are arriving to simplify key IoT security requirements and enable improved functionality.

The IoT SIM Applet For Secure End-to-End Communication (IoT SAFE) is a **GSMA** initiative that allows the SIM to be used as a hardware secure element or root of trust to achieve end-to-end, chip-to-cloud security for IoT products and services. It is widely accepted that the SIM or eSIM (embedded SIM) is ideally suited for this purpose because it offers the best protection against hacking, offers advanced security and cryptographic features and it is fully standardised.

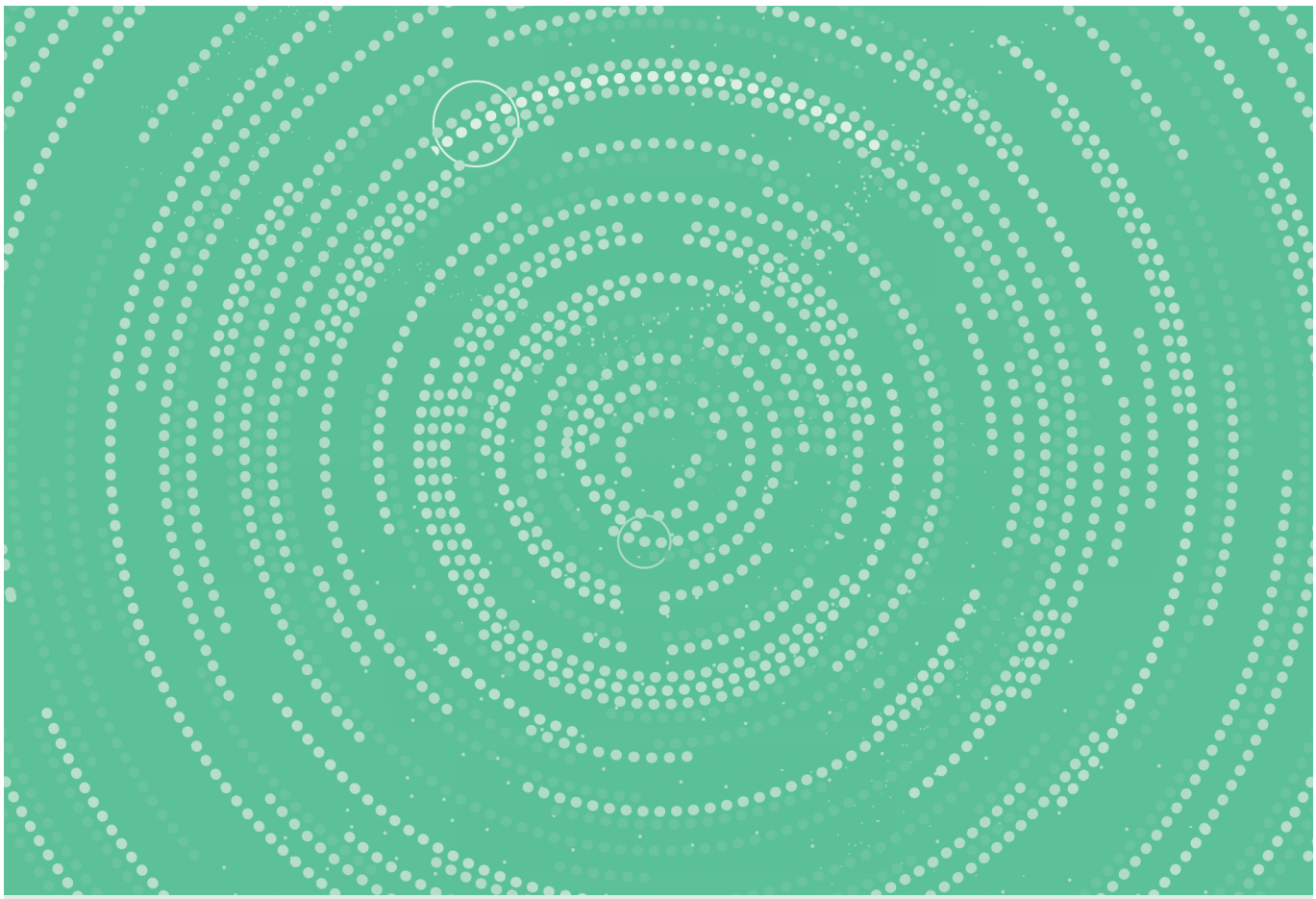
Hardware tamper-resistant elements – with the hardware expressed as an integrated or embedded subscriber identity module (iSIM or SIM) that also contains a secure element - within the device are a standard technology that integrates the new GSMA IoT SAFE specifications. These help to deliver scalable security by design using well-known, proven SIM technology that is already in billions of devices and has been used for decades.

Hardware tamper resistant elements are important because they address the three key IoT security requirements:

1. **Mutual trust between the IoT device and cloud**
   This end-to-end mutual authentication enables a TLS connection

2. **Protection of data at rest and in motion**
   Data integrity
   Data confidentiality

3. **Scalability**
   There are already billions of secure elements in the field ▶



The hardware tamper resistant elements then act as the root of trust and a cryptographic toolbox that stores private keys, digital certificates and security services. IoT SAFE deployment use the SIM or eSIM as a miniature crypto-safe inside the devices to establish a TLS session with a corresponding application cloud/server. IoT SAFE provides a common application programme interface (API) for the highly secure SIM to be used as a hardware root of trust by IoT devices and is compatible with all SIM form factors.

The IoT SAFE applet runs on the SIM/eSIM OS and solves many of the challenges associated with IOT scalability because it enables the IoT device middleware to use the credentials and security in the SIM card for IoT. In essence, the secure element in the SIM/eSIM ties the device identity to the device and assures it as a source of data.

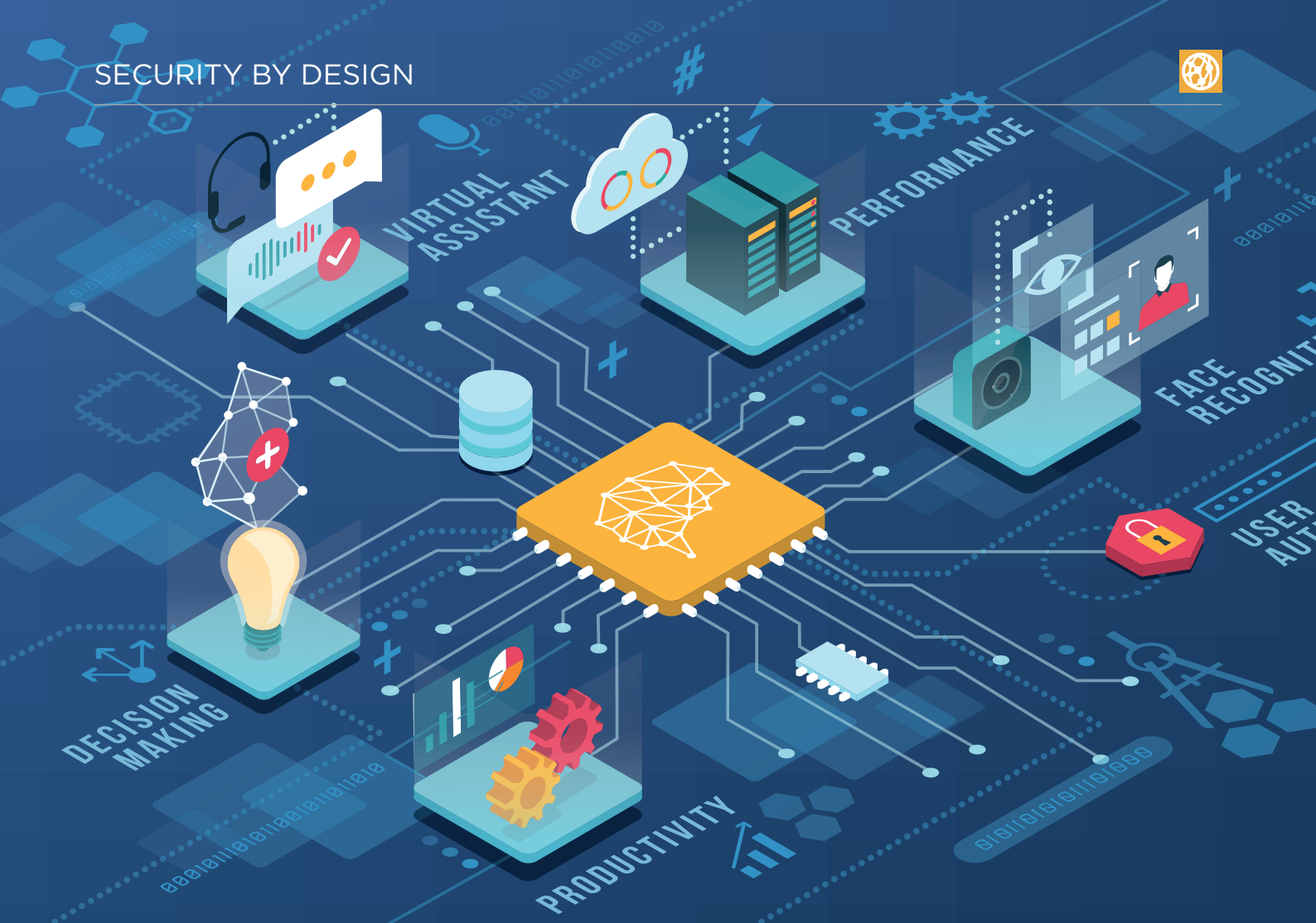
The use case of SIM, eSIM and more recently innovation in iSIM as a root of trust for end-to-end security for IoT products and services is compelling. In particular, eSIM and iSIM enable production, logistical and operational enhancements because there is no need for a physical plastic SIM and iSIM or eSIMs can simply bootstrap a localised connection at their point of deployment which means regionalised product variants are not needed. However, as a root of trust, the SIM becomes the enabler of a secure, trusted device that communicates data in support of whatever use case the enterprise requires.

Conclusion

SIM and eSIM vendors along with chipset manufacturers, cloud service providers and mobile operators have collaborated to develop the GSMA IoT SAFE standard and analyst firms such as Berg Insight expect the standard to gain significant traction this year.

The ability to take a security by design approach and install an IoT SAFE standard-compliant secure element into an IoT device at the point of manufacture addresses the requirement for both a root of trust and flexible connectivity within the device. Coming at the cost of the software for the secure element, the value proposition is attractive. OEMs and service providers are well-placed to roll-out IoT SAFE on behalf of customers with the possibility of creating IoT devices that have 'security inside' on behalf of their customers.

To learn more about IoT SAFE, security by design and the root of trust capabilities of the next generation of SIM technology, visit: **https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/secure-elements/gsma-iot-safe-specifications**

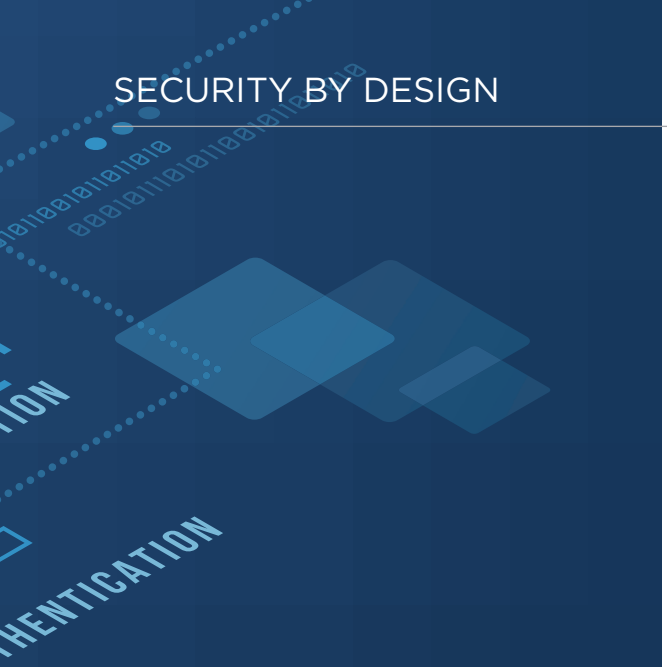


Inside the options and standards behind security by design

The traditional network perimeter is no longer a circle of trust, which is proven by an increase in the cyberthreats and cyberattacks on an organisation. The enterprise network now has to accommodate various devices that are internet-enabled and connected to the network. They include IP cameras, routers, HVAC systems, medical devices, point-of-sale terminals and many more. These devices tend to have limited processing power and storage, leaving little room for conventional security software. IoT devices also often run on older operating systems that cannot be patched, use weak or default passwords, and are not monitored for security breaches, writes Bob Emmerson, a freelance writer and technology editor of Beecham Research

Networking and security teams have historically relied on protections at the network perimeter to secure the entire enterprise. The internal network was deemed trusted and secure. While everything outside was seen as insecure, everything on the corporate LAN was considered to be secure. However, a series of relatively recent developments have resulted in organisations reassessing their approach to security:

- **Digital transformation:** Increased IoT device adoption is helping organisations increase value, productivity and reduce costs.
- **Cloud migration:** More and more devices, managed and unmanaged, are increasingly sending data to the cloud or a multi-cloud environment.
- **Hybrid work:** Employees moving freely on and off the campus network are exposing the corporate network to outside threats. ▶



This resulted in cybercriminals targeting these vulnerable IoT devices and employing them as an entry point into corporate networks. This has become a significant issue. The number of devices connected to IP networks will be more than three times the global population by 2023. This equates to 29.3 billion networked devices by 2023, up from 18.4 billion in 2018.

This is significant not only because of increased cybersecurity risk, in that there are more devices in more dispersed locations, but the fact that in edge computing data processing is exposed to the outside world. Regular network security architectures focus on enterprise data centres but this model is no longer suitable for the dynamic requirements of today's IoT deployments.

It is no longer a question of whether an organisation will be attacked, but when. Unfortunately, many companies still rely on legacy point product solutions, which are inadequate. They cannot detect and respond to advanced attack strategies. Moreover, there is a cybersecurity skills shortage. Relying on manual threat analysis and detection, as well as security-as-you-go strategies, cannot keep pace with the advanced capabilities of cybercriminals.

Zero trust

In 2020, the global pandemic compelled nearly every organisation to embrace a zero trust strategy as employees went remote, virtual private networks (VPNs) were breached or overwhelmed, and digital transformation became critical to organisational sustainability. The mandate emerged for a zero trust approach to verify and secure every identity, validate device health, enforce least privilege, and capture and analyse telemetry to better understand and secure the digital environment. Through supporting thousands of deployments and observing the expanding threat landscape, we have revised and evolved the zero trust architecture and maturity model we released two years ago based on what we have learned.

Zero trust is basically a strategic approach to cybersecurity that secures an organisation by eliminating implicit trust and continuously validating every stage of a digital interaction. It is a conceptual model and an associated set of mechanisms that provide security controls. These security controls do not depend solely on traditional network controls or network boundaries. It requires your users, devices, and systems to prove their trustworthiness, and it enforces fine-grained, identity-based rules that govern access to applications, data and other assets.

"Zero trust is security by design," explains Nicolas Chalvin, the vice president of marketing at **Thales**. "There's no need to provision encryption keys during manufacturing; no need to trust the factory and employ a dedicated security process when injecting key in the devices and transporting them to the IoT cloud provider."

Zero trust principles are intended for an organisation's infrastructure, which includes operational technology, IT systems, IoT and Industrial Internet of Things (IIoT): it's about trying to secure everything everywhere. Traditional security models rely heavily on network segmentation and give high levels of trust to devices based on their network presence. In comparison, zero trust is an integrated approach for verifying connected devices, regardless of network location. It asserts least privilege and relies on intelligence, advanced detection and real-time threat response.

Artificial intelligence

As the modern threat landscape continues to expand, AI is being increasingly employed as part of a security strategy. Given the speed and complexity of modern cyberthreats and the current cybersecurity skills shortage, many network security teams need the assistance of machine learning and other AI-based capabilities in order to detect, secure, and mitigate modern attacks. In addition, they need to understand which AI capabilities they need to begin to incorporate into their security stack now to maintain a consistent security posture while their network continues to evolve and expand. ▶

"Zero trust is security by design," explains Nicolas Chalvin, the vice president of marketing at Thales

IoT devices rely on establishing trust with a cloud to exchange data securely, but there are different proprietary security solutions and this creates fragmentation in the market

Jean-Francois Gros
IoT Product Lines Director
Thales

Nicolas Chalvin
VP of marketing, connectivity and embedded solutions
Thales

However, it should come as no surprise that while organisations are adopting AI to bolster their security efforts, cybercriminals are also adopting of things like agile software development, automation, and machine learning to potentially use AI themselves to better identify and more quickly exploit network vulnerabilities.

Encryption

Security cannot be an afterthought in the design process of IoT devices and solutions. It has to be designed in, not added afterwards. Encryption is one of the most popular and effective data security methods used by organisations. Data encryption translates data into another form, cipher text, so only authorised users can access the data as clear text. While encryption transforms data using a specific algorithm, tokenisation protects sensitive data by substituting non-sensitive data. It creates an unrecognisable tokenised form of the data that maintains the format of the source data.

At a high level, data encryption types can be classified by their position in the technology stack. There are four levels in which data encryption is typically employed. In general, the lower in the stack encryption is employed, the simpler and less intrusive the implementation will be. On the other hand, by employing encryption higher in the stack, organisations can typically realise higher levels of security and mitigate more threats.

A hardware security module (HSM) is a dedicated device that is specifically designed for the protection of the cryptographic keys, which encrypt and decrypt data and perform functions such as signing and verifying signatures and ensuring the integrity of those keys and the cryptographic functions within a secure environment such as an HSM.

Thales HSMs provide high assurance key protection at up to 6,070 transactions per second. They are used to establish a safe and reliable environment for electronic transactions. These public key infrastructure (PKI) based mechanisms utilise certificates and private keys and enhance authentication and encryption security. Moreover they act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organisations in the world.

Root of Trust

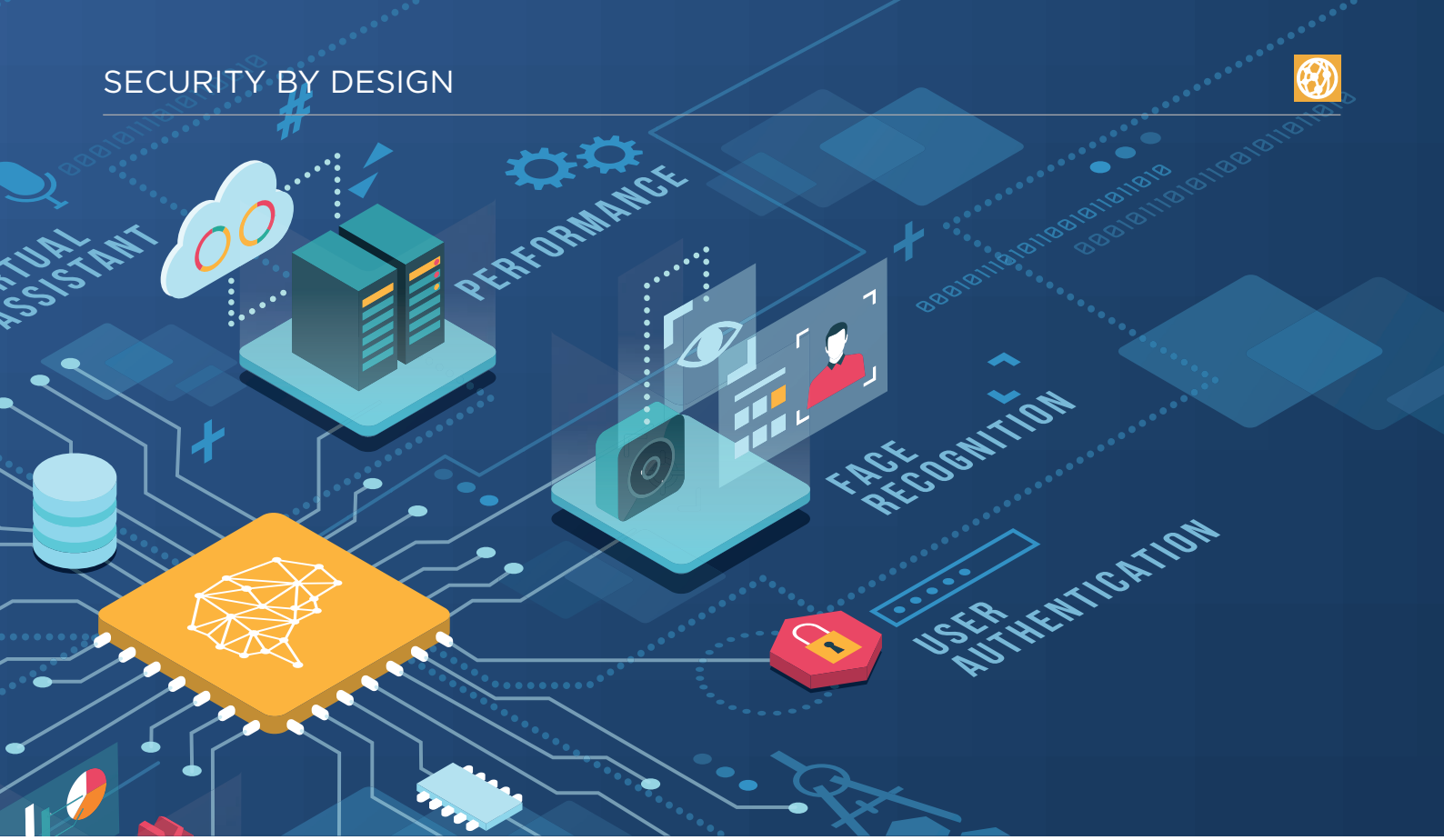
Root of Trust (RoT) is a source that can always be trusted within a cryptographic system. Because cryptographic security is dependent on keys to encrypt and decrypt data and perform functions such as generating digital signatures and verifying signatures, RoT schemes generally include a hardened hardware component.

IoT SAFE (IoT SIM Applet For Secure End-2-End Communication), a relatively new GSMA standard, employs the SIM as the hardware RoT in an IoT device as it has advanced security and cryptographic features. Moreover SIMs are a fully standardised component that can be managed remotely, thereby enabling the provisioning, and maintenance of the credentials and server certificate(s).

IoT devices rely on establishing trust with a cloud to exchange data securely, but there are different proprietary security solutions and this creates fragmentation in the market. IoT SAFE addresses this issue, by delivering a repeatable, standardised, scalable solution. It effectively bakes secure connectivity into the device at the point of manufacture and enables even the smallest devices to connect, authenticate and exchange trusted data immediately with the cloud.

“IoT SAFE has a touchless provisioning feature,” says Jean-Francois Gros, the director of IoT Product Lines at Thales. “After manufacture, when the device is switched on, keys are automatically provisioned. There is no additional security cost. It makes use of the intrinsic security functionality of eSIMs, which are employed on all cellular devices. Moreover, IoT SAFE does not depend on the connectivity. Security is maintained when transferring between MNOs.”

Relying on a hardware secure element, or RoT, to establish end-to-end, chip-to-cloud security for IoT products and services is a key recommendation of the GSMA IoT Security Guidelines. This requires both the provisioning and ▶



use of security credentials that are inside a secure place within the device. The requisite functionality can be built into microcontrollers and application processors. Chip makers combine trusted hardware such as a processing engine, crypto accelerators, fuses, private storage and random number generators with a small amount of trusted software. These trusted functions, and their complexity, are usually hidden behind a software interface so that software developers who are not security experts can employ them.

Intel has announced that it is building security as default into its new platform for IoT device developers: Pathfinder for RISC-V. **Check Point** Quantum IoT Protect will be available in new Intel Pathfinder for RISC-V, enabling IoT device developers to easily integrate cybersecurity without impacting product performance. The move comes as a result of a collaboration with Check Point Software Technologies, a developer of embedded security technology.

PSA Certified is an industry-wide, comprehensive response that is maintained by security experts and backed by over 50 ecosystem partners. It features a Root of Trust developed specifically for IoT and a framework that analyses security threats, architects individual solutions, implements them with trusted components, and finally certifies the result. Everything is aligned with industry and government standards as well as emerging IoT legislation and there are ten documented goals that guide security best practice.

Standardising the Root of Trust

Right now, embedded SIM (eSIM) technology provides a unified approach to global, future-proofed connectivity that can help organisations scale IoT deployments into networks that comprise tens and even hundreds of millions of connected devices. eSIM and the newer integrated iSIMs (iSIM) allow multiple connection profiles per device, thereby providing easier switching between networks plus enhanced security. In addition, over-the-air (OTA) provisioning enables zero touch provisioning at the touch of a button.

Standardising the RoT, within a device's SIM, ensures a common mechanism for secure data communications using a highly trusted and time-tested module. It offers a cost-effective mechanism for cloud authentication and end-to-end security since SIMs are already used for authentication on mobile networks. That makes IoT SAFE a key step towards uniting the industry in realizing the vision of a truly secure IoT, from chip to cloud.

IoT SAFE meets the needs of IoT security for all SIM form factors: SIM, eSIM and iSIM. But in order to maximise IoT security, it makes most sense to bake that RoT directly into the system on a chip (SoC). iSIM takes IoT SAFE further than any other SIM form factor as its existence in a device can be relied upon. This development gives device manufacturers the best way to mitigate potential attacks, and by using a secure, tamper-resistant hardware element to protect credentials, it reduces the risks associated with spoofing or man-in-the-middle attacks when exchanging sensitive data with the IoT service provider's cloud.

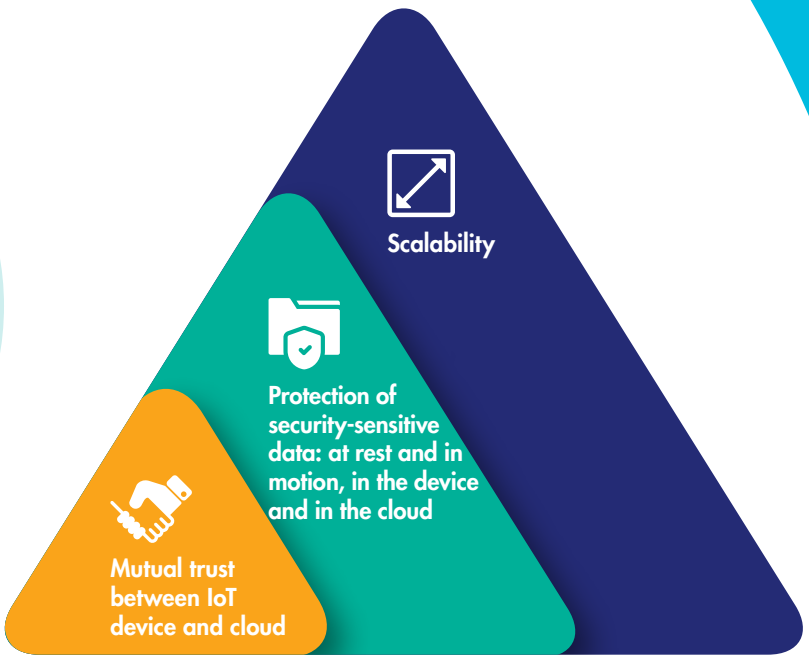
The combination of IoT SAFE running on an iSIM allows for self-contained processing and encryption elements to manage security-related workloads for network and cloud authentication in a more integrated yet tamper-resistant way. It enables a vast new range of secure use cases covering a combination of smaller device sizes, baked in connectivity and seamless provisioning and lifecycle management.

iSIM takes IoT SAFE further than any other SIM form factor as its experience in a device can be relied upon

With Thales IoT SAFE

- Delivers scalable security by design for the IoT
- Leverages hardware tamper resistant eSIM, iSIM or SIM
- Follows the GSMA IoT SAFE standards
- Achieves seamless security with our touch-less provisioning concept: devices are automatically provisioned at first use with no impact on device design and production

Hardware cryptographic toolbox



Benefits for the key stakeholders

MNOs
can offer new secure IoT services and capitalize on their experience with billions of SIM and eSIM already deployed and managed by OTA (Over-The-Air) and remote provisioning platforms

Public Cloud Providers
can offer seamless and secure access to their cloud and minimize the risk of attacks

OEMs
can protect device integrity, streamline production of secure devices and overcome fragmentation

IoT Service Providers and Fleet Managers
can develop secure services once - then deploy and manage the life cycle of their fleets of IoT devices everywhere, regardless of device fragmentation

Thales IoT SAFE

> Thalesgroup.com/Mobile <