thalesgroup.com

THALES

Building a 5G world we can all trust

How Thales is helping telcos maximise revenues and minimise risk in the 5G era

10x more devices can connect per KM² than 4G (1 million devices)

(ETSI)

Trusted 5G

How to connect billions of people and things safely

Unlike almost any other type of organisation, telecommunication providers are best placed to support people's increasingly digital lives. 5G connectivity is unleashing super-fast mobile broadband, ultra-low latency networks, network slicing and the ability to connect billions of devices.

As the world of every consumer and every enterprise becomes increasingly digital, there is huge opportunity for telcos. A hyper-connected world will encourage a shift away from selling low-margin connectivity towards more personalised and profitable analytics-driven experiences.

There is a 'but'…

New vulnerabilities are emerging.

Cyber security attacks are becoming more sophisticated.

Unease over data privacy continues to grow.

Key concerns for telcos

Virtual network infrastructure

The 5G core network is almost exclusively cloud-based. Carriers are unable to protect it in the same way as the largely physical networks that came before.

An unprecedented volume of data

The 5G era will see a huge upsurge in the volume of data at rest and in transit. As interconnections increase too, this data is at threat. Customers will expect telcos to protect individual and corporate information.

Millions of new connections

5G promises to connect millions of IoT devices with lightning fast speeds. However, this market will also attract OEMs with no history of network security, identity or key management. Placing an ever-greater burden on telcos.

New ground

In a 5G world, enterprises will be able to leverage further the possibility offered by private networks. This could by leveraging network slices.

Meeting customer expectations

Many telecom operators still onboard customers via bricks and mortar stores. Without innovation in this area, the telco market is ripe for the kind of disruption seen elsewhere.

The digital divide

Billions of people around the world live in regions with little high-speed internet access. Demand is high for voice and data services. Yet installing the infrastructure to provide it remains an expensive challenge for telcos.

Despite working with these issues every day, telcos still need expert external support to realise the opportunities and navigate the challenges of our increasingly connected world.


5G will
account for
21%
of total mobile
connections in 2025
with 1.8 billion users
(GSMA Intelligence)

5G is coming

Digital transformation is accelerating

In June 2017, the European Space Agency revealed the Satellite for 5G Initiative. The paper outlined how non-terrestrial networks could bring 5G to even the most remote corners of the planet.

The news was highly significant for telecom operators. Why? Because analysts believe connecting the 750m people living in unconnected areas could deliver $3.8bn in annual wholesale revenue. Moreover, connecting existing subscribers travelling to remote areas could bring in $6bn a year.

Non-terrestrial networks (NTNs) can unlock this revenue – and enable an Internet of Things that spans every inch of the earth.

Why mention this in a 'Thales for telcos' paper?

Because Thales was one of the 16 signatories to the ESA statement -contributing to the definition of the NTN standards, running the trials and launching the satellites.

But the NTN division is just one facet of Thales' commitment to the mobile industry. We could have chosen any number of specialisms to open this paper with: SIM technology; high speed encryption; hardware security modules; IoT modems and more.

What Thales brings to Telcos

The outlook for Mobile Network Operators and Communications Service Providers will be dependent on the response to the challenges and opportunities of the emerging 5G era. Thales believe these factors can be clustered into three key considerations:

Connect

"How can we connect exponentially expanding groups of people and things?"

Protect

"How can we protect our customers, our networks and our data from cyber attacks?"

Predict

"How can we predict events using analytics to make us more efficient and profitable?"

Trusted Tech by Thales

Helping connect, protect and predict in a 5G world

Connect

"How can we connect exponentially expanding groups of people and things?"

Protect

"How can we protect our customers, our networks and our data from cyber attacks?"

Seamlessly migrating subscribers to next generation network, while keeping their privacy safe

Billions of people will be moving to 5G over the next few years. Their interactions with service providers are moving away from physical stores and are progressively moving into the digital sphere. This brings challenges when onboarding new users remotely, requiring simple connectivity set up and management for all of their devices. Telcos will need support to manage growing numbers of subscriptions, SIM fleets and the broader device ecosystem. New processes are required to smooth logistics.

Deploying trusted connectivity for billions of devices

How do we connect all of these devices? Both smoothly and securely requiring remote on-boarding and de-activation. They will need to be connected to a variety of network technologies. Many of these devices will be small and battery powered calling for miniature, lower power connectivity while others need to last for many years or be resilient to survive in a harsh environment like under the hood of a car. Through private networks, enterprises gain communications autonomy but this brings new challenges around subscriptions and IoT connectivity.

Connecting the unconnected

New satellites can bring 5G services to the 750 million people who currently live in unconnected areas and deliver billions of dollars in new revenue. Non-terrestrial networks will help unlock this revenue, while enabling IoT in any area in the world.

Securing devices and access management

5G networks are similar to other cloud networks – and can suffer the same types of cyberattacks. All parts of the network need to be cybersecure. This includes the device, access to the network and corporate resources as well as the data and cloud itself. This calls for a rigourous process that starts with security by design and ends with threat detection for the most critical resources. And when we look at IoT, if there are tens of billions of machines on the network, how can we stop them from being compromised – and how can we trust the data they send?

Protecting the cloud (and the edge)

Cloud-native virtualization brings new security risks. When a network resides in the cloud, there is a danger of cross-contamination and data leakage. The pressure is on telcos to deliver strong encryption of data – and accurate authentication of those given access to it. Encryption is not only needed to secure data but also to help telcos comply with a growing number of privacy regulations.

Detecting threats, protecting enterprises and critical infrastructure

Enterprises gain autonomy and agility through private networks. But, their private cloud also needs protecting. Corporate devices and sensitive data on public networks also need protecting from device loss, theft or eavesdropping. Guidance, tools and techniques may be needed to enable enterprise customers to scrutinise their core systems, encrypt everything and apply a security by design approach. Yet no system is 100 per cent secure. There will be always be some vulnerability. To reduce this uncertainty, one strategy is to monitor the network for anomalies, detect threats and counter them.

How Thales has evolved

In 2019, Thales acquired Gemalto – the culmination of €7 billion worth of investment in digital technologies in recent years. The expanded Thales Group is now set up to provide telcos with a wider range of digital identity and security, software, data processing, real-time analytics, connectivity and end-to-end network management services.

Predict

"How can we predict events using analytics to make us more efficient and profitable?"

Gaining insights from an uncertain consumer context

Mobile networks already generate huge amounts of data. With 5G, data volumes are certain to grow exponentially alongside the rapid uptake of 5G connectivity. Telcos needs a new way to analyse all this data. 5G analytics enables telcos to gain deeper insights from such a wide range of information. Insights are needed throughout the customer lifecycle and AI helps to interpret a multitude of signals. This starts with automated fraud detection when onboarding users as well as studying people's digital interactions with the network to devise more effective promotions.

Anticipating network anomalies

5G network data is strategically valuable. It can be analysed to improve customer service and to diagnose and fix operational issues. The core of a Telco's service involves keeping the network running optimally. 5G incorporates automated solutions to optimate operations and flag network problems. Machine learning helps do this and deliver predictive maintenance rather than waiting for an issue to arise.

Predicting growing numbers of cyberattacks

As critical infrastructure providers telcos need new ways to understand massive quantities of data and constantly analyse the cyber attack threat level, and adapt its line of defence. To ensure protection from cyber attacks, cybersecurity centres can be implemented to monitor network infrastructure around the clock.

As you will see in the pages that follow, across each of these areas **Thales is making the new world of telecommunications a place we can all trust.**

Where to start?

In the sections that follow, we showcase the ways Thales will help you connect, protect and predict across five of the most critical issues affecting telcos today:

The telecom industry faces

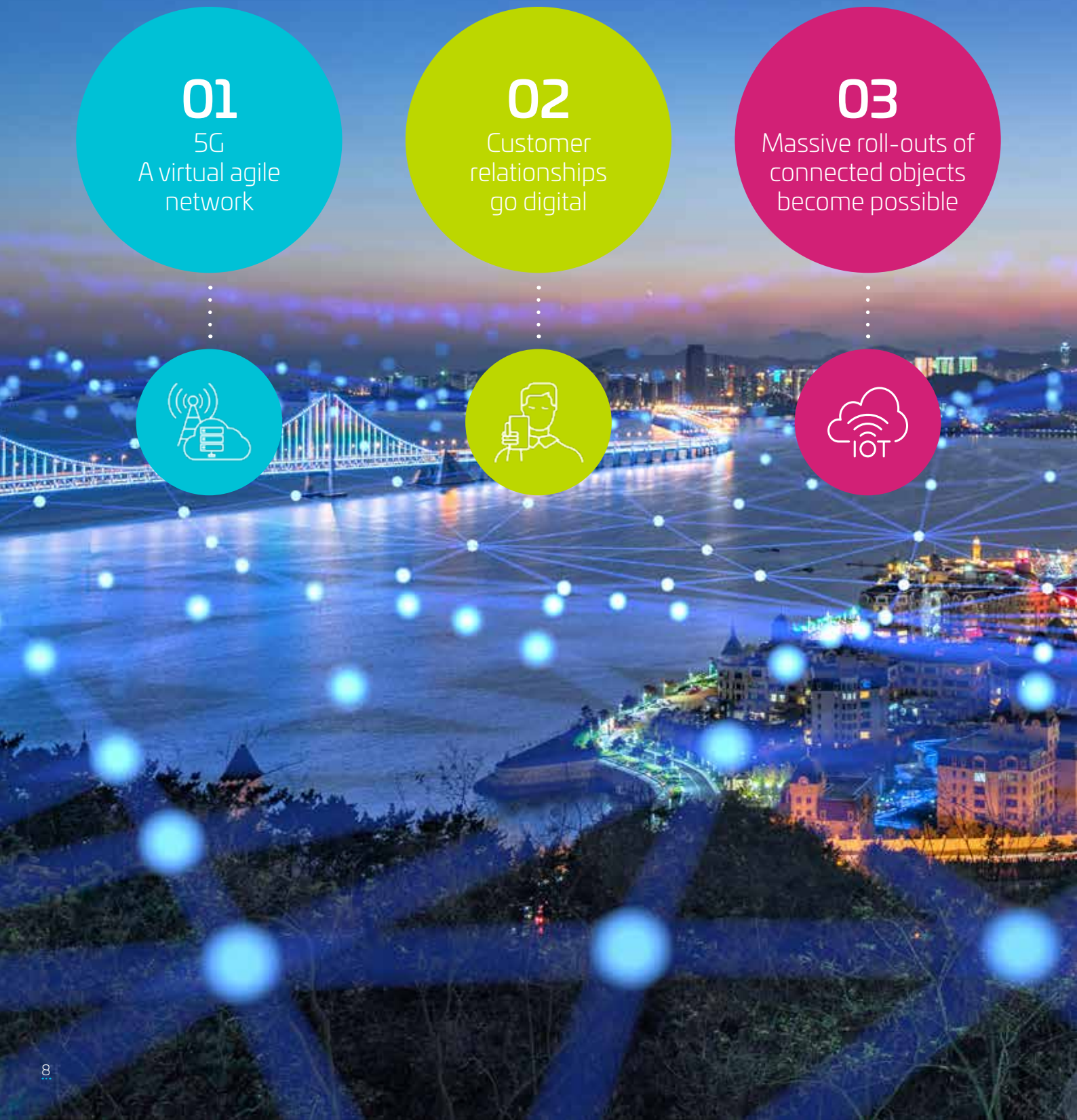
5 new challenges

and so many opportunities.

01
5G
A virtual agile network

02
Customer relationships go digital

03
Massive roll-outs of connected objects become possible




04
Enterprises gain communications autonomy
05
The data-driven network must be cybersecured

New ways to overcome the risks and enjoy the rewards of 5G

The 5G network is unlike its 2G, 3G or 4G predecessors. It brings exponential improvements in speed, latency and reach. Becoming virtual, the core network can now adapt to all use cases.

Over the last two decades people have grown used to the idea of mobile network upgrades. They expect incremental improvements every few years and many of them will think the same way about 5G: That it is just a slightly faster version of 4G. It is not.

5G will create new opportunities for people, enterprises and societies by enriching consumer experiences, speeding up digital transformation and advancing civil interactions.

5G will accelerate the adoption of IoT. Connected objects will be able to power on for years without human intervention. This will dramatically reduce the costs of connecting billions of devices. It will also introduce digital transformation to 'analogue' industries like mining or agriculture.

All of this represents a huge commercial opportunity. So telecom operators are having to invest – and invest heavily – in new 5G infrastructure. Thales understands what is required in a 5G world defined by cloud-native virtualization, software-defined networking and network slicing.

Connect

Thales offers a broad range of SIM products and secure elements to connect people and things. We also help telcos to manage their SIM fleets and device ecosystems making it easier to on-board and de-activate remote devices. Now, as we enter the 5G era, Thales is working hard on new IoT modules and SIM form factors more appropriate for machines and sensors.

How Thales is supporting wider 5G coverage

By teaming up with Thales, telcos can create non-terrestrial networks with greater coverage for hard-to-reach communities, outdoor IoT devices or moving platforms.

The 3GPP standards body has issued a series of releases to support the development of satellites based on the same technology framework as 5G. The leadership of Thales Alenia Space has been instrumental in the adoption of the Non-Terrestrial Network in 5G, and the work is now underway for the normalisation. To provide direct access to 5G mobile services, the satellite industry will follow this with low earth orbit vehicles from 2024.

This is where the Thales 5G SIM comes in. In 2019, Thales launched the world's first 5G SIM. It introduces three additional benefits to traditional SIMs:

1. **Subscriber identity privacy**
   The 5G SIM computes the Subscription Concealed Identifier (SUCI) to anonymise the Subscription Permanent Identifier (SUPI) which has replaced the IMSI. It ensures full end-to-end subscriber identity anonymisation, under the control of the telco. It will comply with the highest security requirements imposed by local 5G regulations.
2. **Cyber resilience**
   While 100% safe as stored into the SIM, sensitive network access authentication data can be unexpectedly or accidentally exposed outside the SIM. 5G SIM can restore or build a trustful security level all over the subscription lifecycle without reissuing new SIM cards with the capability to change credentials and algorithm upon the telco request.
3. **Enterprise confidentiality**
   With Thales' portfolio of SIM (rSIM, eSIM) and High Speed Encryption (HSE) solutions, telcos can add higher levels of confidentiality to 5G private/non-public networks. They can also tailor security, authentication and authorisation for each network slice.

The virtualized network also calls for robust cloud and data protection. Our CipherTrust Data Security Platform helps any organization to see where its data resides, and then classify it. Thereafter, the enterprise can use the platform to encrypt or tokenize the data – and safely manage the access keys.

Protect

How Thales is helping secure 5G networks

5G networks demand new ways to identify people and objects accessing the network due to three factors:

1. **Compliance with new data privacy**
1. **regulations and stronger security requirements**
2. **Increasing cyber attacks against mobile networks**
3. **Greater attack surface for 5G virtualised networks due to IoT**

Predict

How Thales is pioneering 5G analytics

In 2017, Thales acquired Guavus – a leader in the field of big data processing and analytics. For telcos, the Guavus 5G Analytics portfolio supports rapid digital transformation by applying processing and predictive analytics to vast quantities of data.

The **Guavus-IQ** capabilities provide a multi-perspective analytics experience for telcos, delivering actionable insights in real time. As a result, operators can identify subscriber behavioural usage patterns and better understand network operations. This enables them to increase revenue opportunities through data monetization and improved customer experience, as well as reduce OPEX through automated, closed-loop actions.

$1.1 trillion

Expected investment from telcos between 2020 and 2025 – 80% allocated to 5G.

(GSMA Mobile Economy report, 2020)

$2.2 trillion

Estimated value that 5G will add to the world economy by 2034

(GSMA Mobile Economy report, 2020)

Towards a 100% digital customer relationship >>

Managing the shift towards a 100% digital customer relationship

On-boarding. After-care service. Promotions. These customer interactions will not only take place in (fewer) physical stores but also into the digital sphere. Whether driven by the global health situation or individual preferences, people are increasingly likely to explore online options. At the same time, a rise in ecommerce and video conferencing is driving a rising demand for connectivity services.

Telco-branded high street stores and customer care will remain a significant touchpoint for many consumers for some time to come. But a major shift to digital channels is inexorably taking place as digital natives and 'digital immigrants' are switching to a mobile app-first experience only.

As the customer relationship moves online, Thales is helping telcos maintain a digital connection with customers, improve digital security and generate insights from the new raft of data being created.

50x
more digital interactions in 2025 than 2010

Connect

How Thales is enabling digital customer journeys

The Thales eSIM can be pre-integrated into a device. This dramatically simplifies and streamlines the distribution of mobile subscriptions.

eSIMs make it easier to connect all types of devices. From phones and smartwatches to PCs, tablets, fitness bands or connected cameras. Even industrial machines like smoke detectors, connected cars or smart meters. These tools simplify logistics for OEMs over the lifecycle of each product.

Once a customer has signed up for a connection or service, the onus is on the telco to make the experience as good as possible. This is challenging in an ecosystem that has to support thousands of phone OEMs and firmware variations. Thales eSIM management solutions will overcome these barriers. As soon as a new device is added to the network, Instant Connect automatically and remotely configures the operator settings.

Protect

How Thales is providing trusted digital on-boarding

People are well used to the idea of a digital ID. They have email addresses, social media aliases and more. Yet digital identity can be 'slippery'. People can have dozens of email accounts, for example.

This is why a trusted digital ID matters so much. Thales Trusted Digital Identity platforms capture and verify a subscriber's information from an identity document – a passport, driver's license, or national ID – as well as unique biometric data to verify their identity.

For telcos and other enterprises, this level of trusted digital identification leads to smoother workflows, faster customer acquisitions and consistent consumer data.

Predict

How Thales is improving end user experiences through analytics

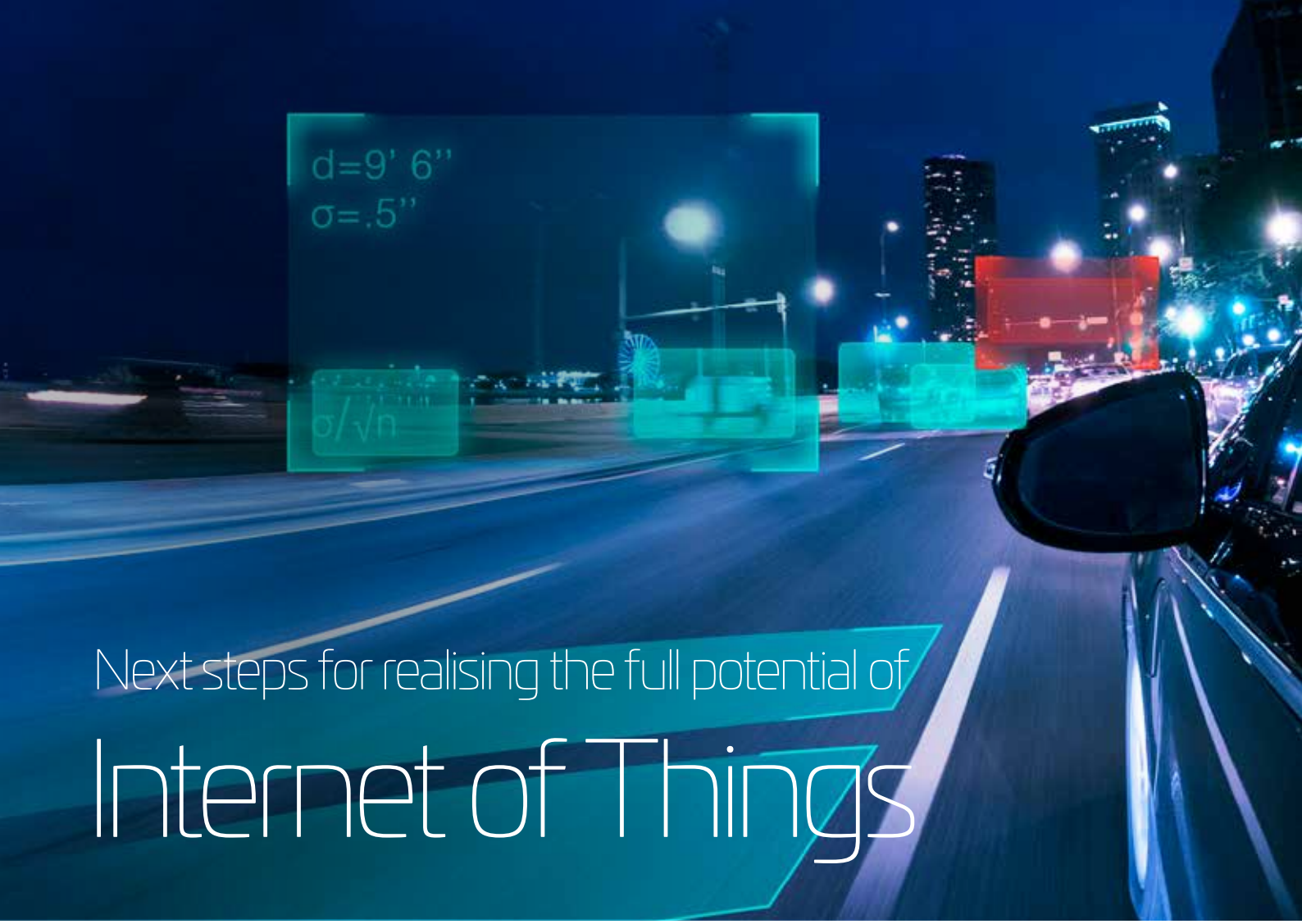
Today's mobile networks already generate vast quantities of data. With the introduction of 5G services, these data lakes will rapidly expand. This data is still extremely valuable. Telcos can analyse it to improve customer services (and boost ARPU) as well as to diagnose and fix network issues.

But this can prove difficult. Especially when it is hard to source, capture and store all this data before attempting to draw meaningful insights from it. Guavus, Thales' telecom analytics arm, develops analytical tools that can handle a typically heterogenous network environment.

Guavus-IQ is a portfolio of AI/ML-driven analytics capabilities designed to provide highly instrumented insights into Telco subscriber and network behaviour. Guavus-IQ consists of two categories of analytics solutions:

- **Guavus Service-IQ** enables marketing operations and product teams to better understand subscribers. By analysing subscriber and device digital behaviours, it offers new ways to micro-segment targets and devise more effective promotions.
- **Guavus Ops-IQ** supports network self-healing through Machine Learning (ML). Designed for network, service and customer care teams, it initiates actions that prevent service degradations or outages from affecting customers.

Realising the full potential of IoT >>



Next steps for realising the full potential of Internet of Things

Connecting machines is a huge opportunity for telcos. Yet it comes with technical challenges that are very different to connecting people and smartphones.

The majority of IoT devices will be small, low-cost, battery-operated and limited in processing power and storage. They might be located in harsh environments and expected to run for decades. This means they need to be configured to act on commands sent remotely.

Telcos will need to ensure that they and their enterprise customers can easily set-up, secure and draw data from a significant number of IoT devices. OEMs and developers will need to examine connectivity options to find the best match for each use case. Some IoT devices will require low bandwidth over short distances. Others may need short bursts of high bandwidth over a much longer range.

Choosing the right IoT connectivity module will ease development, speed up time to market and improve ROI from these deployments. That is why Thales created a broad portfolio of IoT SIMs, embedded SIMs, management and security tools plus Thales Cinterion IoT modules to suit every scenario.

200 million

Chipsets were shipped worldwide in 2019 (Eurosmart). By 2024, there will be an estimated 2.5 billion eSIM-enabled devices

(ABI Research)

Protect

How Thales is bringing security to IoT

Thales eSIMs help telcos protect IoT devices from a growing number of cyber attacks. Since some device manufacturers do not build security into their products, Thales eSIMs offer a new layer of defence.

Thales eSIMs provide a secure element that is highly resistant to cyber attacks. They are soldered into place, making them tamper-proof and harder to physically remove. Each Thales eSIM complies with GSMA IoT SAFE standards. And with a Radio Policy Management platform and an On Demand Connectivity platform, it is easier to remotely and securely manage subscription profiles on individual devices.

Connect

How Thales is supporting IoT subscriptions

Connecting IoT devices comes with a new set of challenges. From device fragmentation to exposure severe operating conditions (temperatures, vibrations etc) to connectivity provisioning. The Thales eSIM was designed to address these issues. Fleet managers can manage, load, delete and replace subscriptions remotely. eSIMs are re-writable, standardised and interoperable across all carriers.

However, IoT subscriptions are unlike personal device subscriptions. They demand new on-boarding and de-activation processes. And with hundreds of IoT vendors instead of a handful of phone manufacturers, telcos need eSIM management tools to navigate this new complexity.

eSIM management suite simplifies device connectivity with everything ready at power on. Thales eSIM management tools include high-speed telco profile downloads over HTTP, standardised APIs for back-end integration and subscription profile swap or termination. Together they can smooth the logistics process for telcos and OEMs.

The next advance: iSIM

Integrated SIM (iSIM) technology places iUICC functionality directly into the chipset called system-onchip (SoC). This will further reduce the space and power consumption, while keeping the highest security requirements for eSIM. Thales is currently working with Qualcomm to develop iSIM technology in the Snapdragon chipset.

Predict

How Thales is improving IoT analytics

Thales is creating a new generation of advanced analytics services for 5G-enabled IoT devices. These devices require constant monitoring to be able to send back valuable data from the network 'edge'. The ultimate goal is to create a 5G operational environment in which machines are able to fix themselves. Until that point, Thales machine intelligence is enabling telcos to streamline and automate human workflows.

Telcos can apply the Guavus Ops-IQ service to analyze big data from IoT devices in real time. This can be used to take decisive actions to increase network efficiency or to fix a specific hardware or software problem before it has a wider (and more costly) impact.

Delivering a new wave of possibilities for enterprise customers >>

Delivering a new wave of possibilities for enterprise customers

The role of private companies in the telco market is changing. Instead of passive consumers of connectivity, they are now actively connecting millions of devices and machines. In some cases, they are even running their own 5G private networks.

These new enterprise use cases are only possible after resolving critical questions around identity and security. Private networks – like the one pioneered at the Mercedes Benz car production plant in Sindelfingen, Germany – generate highly sensitive data. This must be encrypted both at rest and in transit and only authorised personnel should have access.

Meanwhile, the growth of IoT requires new and very specific skillsets. Private enterprises will be looking to telco partners to share best practice and support digital transformation initiatives – whether at people's desks, in the factory or out in the field.

Thales has the experience, products and services to help telcos manage these new enterprise customer connectivity, security and identity requirements.

29

different cloud services are used in the average organisation

(2020 Thales Data Threat Report)

Connect

How Thales supports cloud access for end users

The obvious defence is to ensure that employees use strong authentication when they log in to these services. This is not so easy in practice. As the number of cloud subscriptions grows, employees lose track of their many usernames and passwords. Or they use weak ones, which increase the risk of a breach.

Thales SafeNet Trusted Access provides the answer. As a central access management system, it enforces the appropriate level of authentication and applies cloud single sigh on via centrall managed access policies.

SafeNet Trusted Access validates every individual user and can decide whether to admit access to a application or system. It also provides data-driven insights on users. It offers the broadest range of authentication methods, including PKI, OTP Push, email/SMS notification, pattern-based authentication and adaptive/contextual authentication.

Protect

How Thales provides enterprise-grade security

Virtualized 5G networks need a solid cloud security and data protection solution in place using Hardware Security Modules (HSMs) for example. Our CipherTrust Data Security Platform helps any organization to see where its data resides, and then classify it. Thereafter, the enterprise can use the platform to encrypt or tokenize the data – and safely manage the access keys.

Ercom is a Thales company that has developed Cryptosmart – a new mobile security service that enables telcos to address enterprise customer concerns over mobile security.

Cryptosmart is designed to protect the people and mobile devices they use to communicate high-value information. It transforms consumer mobile devices into true extensions of a Restricted Level network. This government-grade security can be deployed on standard smartphones within minutes. Using Cryptosmart, telcos can offer organizations the ability to protect corporate devices and sensitive data on public networks and in the event of device loss, theft or eavesdropping.

Predict

How Thales helps detect attacks before they happen

It is important to protect all devices and data. Yet no system is 100 per cent secure. There will be always be some vulnerability. To reduce this uncertainty, one strategy is to monitor the network for anomalies.

Thales Critical Information Systems (CIS) consultancy provides telcos with the guidance, tools and techniques to enable enterprise customers to scrutinise their core systems. In the past, only governments, defence contractors or aviation firms required this level of protection. But 5G and IoT is changing this.

Thales CIS consultancy performs a deep analysis of information networks to determine the extent of any vulnerabilities. It runs Vulnerability Assessments (VA) and stages simulated attacks to reveal worst-case scenarios. It can even set up a staffed security operation centre to monitor threat activity 24/7.

Ensuring the data-driven network is cyber secure >>

Ensuring the data driven network is cybersecure

The telco industry has a proud record of deterring cyber attacks. Yet the arrival of a new virtual 5G core, private network slicing and the rapid growth of IoT connections will bring new challenges.

Cloud-native virtualisation makes network requirements more complex. The security risk rises as data is shared across the virtual infrastructure. 5G also widens the attack surface for cyber criminals who are well-resourced. So 5G security will need to combine built-in encryption on the (NR) radio interface and end-to-end protection from the device to the corresponding cloud app.

Thales can help telcos and their customers overcome the five major security challenges of this new era:

1. **Network virtualisation** that creates a higher risk of cross-contamination that exposes sensitive data.
2. **Key functions going to the edge** that requires new security capabilities, like Bring Your Own Encryption.
3. **Shifting from proprietary to standard** hardware that makes it easier for malicious actors to infiltrate networks.
4. **Resource sharing between telcos and enterprises** that demands a robust strategy to ensure proper isolation of data.
5. **Zero-touch automation** that lacks the human oversight to prevent automatically triggered negative events.

By 2021, 50%
of data outside of physical control of enterprise IT
(Gartner)

Connect

How Thales ensures data is secure yet available

Encryption keeps data safe. If the data is stolen, it is unreadable. At some point, however, an individual still has to decrypt it so it can be used. This individual will be given a key. If this key falls into the wrong hands all that data is available to the hacker.

Many data encryption systems only store these keys locally. Or do not store the key at all because it is generated as needed from a passphrase. Best practice is to set up an external key management system.

These systems place keys inside a hardware security module (HSM). Each HSM exists outside the computer ecosystem to provide a high level of physical security. However, telcos and enterprise customers are now migrating to cloud environments. This can limit the functionality of some HSMs.

So Thales has created centralised key management systems that separate keys from data in the cloud. They also provide the option for multiple keys (for different files or backups) as well as lifecycle key management.

Protect

How Thales encrypts data at rest and in transit

Encrypting data at rest and in transit is crucial to nullifying certain cyber attacks. Yet some companies still do not do it. Thales is helping telcos ensure encryption is a priority at a time when in-country regulators are increasingly focusing on data privacy.

A complementary technology is tokenisation. This protects sensitive data by substituting it with an undecipherable token, which can be stored in the same size and format as the original data.

Device protection will protect data at rest with encryption on the physical hardware. Telcos can then use the Thales CipherTrust Data Security Platform and High-Speed Encryption (HSE) to protect data moving over networks.

Predict

How Thales analyses cybersecurity threats

5G is the first mobile generation to have a natively virtualised network. And, it is launching in a period of growing cybercrime rates. As it will be a driver for every industry, undisputable security and resilience are required. The cyberattack techniques that have emerged in recent years are increasingly complex and hard to detect. Most detection systems are based on rules derived from well-known attack patterns. And cyber threat hunting, which consists in proactively searching through networks to detect hidden advanced threats, is usually performed on an occasional basis. Thales has developed Cybels Analytics, a comprehensive and advanced attack detection solution. Based notably upon machine learning algorithms, it provides both real-time threat detection and hunting capabilities around the clock to help telcos' cybersecurity analysts spot the most advanced threats. Integrated into the Telco's Security Operations Centre (SOC), it reveals three times more attacks than conventional attack detection tools and reduces the time taken to detect advanced, persistent threats from months to days.

What next? >>

Delivering successful 5G services

The deployment of virtualized 5G networks marks a step change for the telecoms industry. It is a game changer, not only in terms of business opportunities but also in the skills required to connect and protect billions of people and things. This will generate unprecedented amounts of data and raises a vital challenge; how to guarantee the security and privacy of data while creating value from it.

Why Thales?

We combine decades of experience in cellular and satellite connectivity with cybersecurity and AI expertise. Our global offer for telcos brings trust to 5G services and our 80,000+ people in 68 countries help to:

- Serve 450 mobile network operator customers
- Deliver cybersecurity solutions to the top 5 cloud service providers
- Define 5G communications satellites

Trusted 5G by Thales

Connect. Protect. Predict.

www.thalesgroup.com/trusted-5G

THALES

Building a future we can all trust