



Securing 5G's future

Why cybersecurity is key to realising
the full promise of 5G networks



Contents

Executive summary: Combining opportunity and security in the 5G world	3
Entering the 5G era.....	4
Resilience by design.....	8
Likely 5G use cases in Switzerland	11
How Swiss 5G pioneers can build trust into the system	14
Conclusion: Seize the 5G moment through trust, resilience and enablement.....	18

Executive summary

Combining opportunity and security in the 5G world

Across the world, connected devices are changing how people live and work. The communications networks that link these devices and enable them to talk to one another are integral to this evolution. In this context, the roll-out of faster, higher-bandwidth 5G networks is a significant step forward — but one that also needs to be kept in perspective. Despite the hype surrounding 5G, the reality is that many of the services that it will enable have already been provided through its 4G predecessor and various low-power wide-area networks (LPWAN).

That said, the technology underlying 5G marks a break with the past in some important ways, including a fundamental reconceptualisation of what a communications network looks like. The previous four generations of mobile technology were founded on physical architecture. Although 5G includes new hardware, it is first and foremost a virtual network — finally turning the convergence of networks and wireless communication into reality. This breakthrough will unleash a wave of innovation, but the greatest impact will perhaps be felt through new or enhanced uses of wireless technology. These may include Fourth Industrial Revolution (4IR) infrastructures, smart cities, autonomous vehicles, remote surgery and new, more powerful artificial intelligence (AI) systems.

Today, this is happening against the backdrop of the COVID-19 global health emergency. Because many governments have enacted various stay-at-home orders, larger numbers of people will be working from home via communications links that are increasingly based on 5G networks. Companies that are more advanced in their digital transformation are telling us that their investment in technology, cybersecurity and resilience has paid off as they respond to the novel coronavirus.

But these shifts have also placed intense scrutiny on cybersecurity. Some commentators have suggested that 5G networks increase the potential attack surface for cyber adversaries, because 5G connects many more devices than previous technologies and uses distributed processing power ‘at the edge.’ However, many of 5G’s anticipated vulnerabilities result from other elements of the 5G ecosystem — notably the security of the end devices. The good news is that the challenges to cybersecurity in 5G networks can be overcome, providing a solid basis for innovation by parties worldwide to deliver the full promise of this technology.



Entering the 5G era

We are on the threshold of a world supported and connected by 5G-enabled massive Internet of Things (mIoT) capabilities. In this world, 5G helps to provide the bedrock for our smart cities, our 4IR operating models, our smart homes, our smart transportation, our smart healthcare and myriad other potential use cases. PwC's recent paper [*The Impact of 5G: Creating New Value across Industries and Society*](#), published in conjunction with the World Economic Forum, articulates the wide range of existing 5G use cases that are already transforming the business environment.

As with any new technology, the introduction of 5G requires us to revisit our approach to cybersecurity. However, this need should not distract the organisations, governments, cities and industries planning for the 5G revolution from the significant opportunities it offers. In fact, by understanding and countering the risks specific to 5G, companies can build greater resilience, and use 5G as a powerful force to generate revenues and profit in their businesses and good in society. This has become even more imperative today, as the coronavirus pandemic changes how people live and work in unprecedented ways.

When it comes to why 5G is different, the numbers speak for themselves. In combination, its technical attributes — as summarised in “The technical attributes of 5G,” on page 5 — mean 5G is capable of achieving speeds approximately 100 times faster than 4G and handling significantly more connections. These advantages are amplified by ultra-low latency — the time it takes to receive a response to a request.

Although consumers are excited by the prospect of downloading ultra-high-definition (UHD) movies in seconds, the true benefits of these technical attributes will manifest themselves through a wide range of innovative applications. These may well change not only how we entertain ourselves but also how and where we work, how we move around, and how we keep ourselves healthy — with AI-enabled personalisation embedded in 5G applications playing a growing role in helping us do these and other things.

The ability of 5G to deliver on its promise is rooted in its being a software-enabled network that's operated through distributed digital routers and optimises processing speed and power by relocating operations to the fringe. This contrasts with the 'hub and spoke' configuration of previous generations of mobile technology.

The 'zero trust' approach

Keeping 5G networks secure will be key to realising the full potential benefits for consumers, businesses and entire societies alike, and for ensuring the safety of end users. This has become all the more critical during the coronavirus pandemic, as more and more companies adopt remote working policies and as telemedicine use increases. For example, with staff working outside the office, companies' IT infrastructure systems are being stretched, creating heightened vulnerability to cybersecurity attacks. And as patients connect with medical professionals via their tablets, laptops or mobile phones, sensitive information will need to remain secure.

A vital first step towards protecting any network against cyber threats — 5G included — is to understand where vulnerabilities might arise. This is primarily at the points of interconnection, where risks transition from one element of the network to another. With 5G, as with 4G, different companies are often involved on each side of these transitions, meaning a coordinated approach is vital to ensure security is effective from end to end. The approach also needs to be agile, given that technology tools are advancing rapidly, and both companies and cybercriminals seek to use them to their advantage.

All participants in the 5G ecosystem — including mobile operators, network vendors, system integrators and end businesses — should agree to identify, profile and assess the health of every component before it's permitted to connect to the network, and, if appropriate, limit access to the 5G service based on this assessment. This can be achieved with a strategy grounded in the following elements:

- 1. Zero-trust approach**
- 2. Universal encryption**
- 3. Orchestration by AI**

The technical attributes of 5G

5G brings significant changes to many aspects of the network — including core and management systems, as well as all protocol layers ranging from radio to applications. Its technical attributes include:

- **Network slicing**, which provides a way for service providers to enable network-as-a-service (NaaS) to specific subscriber groups, giving them the flexibility to manage their own devices and services according to specific needs
- **Enhanced mobile broadband (1–20 Gbps)**, which supports applications such as 3D video transmissions with 4K or 8K resolution screens, online gaming and so on
- **Ultra-low latency (<1ms)**, which is important for mission-critical services such as augmented reality (AR) and virtual reality (VR), telemedicine and healthcare, intelligent transportation, and industry automation
- **Massive device connectivity** for vehicles, mobile subscribers, enterprises, IoT and the like
- **High availability and dense coverage**, which will make it capable of providing unlimited connectivity for billions of different subscribers
- **Low energy consumption**, with up to ten-year battery life for M2M (machine-to-machine) communications.

To deliver these capabilities, 5G is equipped with a new air interface that supports heterogeneous access networks and handles variable bandwidths. Packet core network upgrades are also being implemented, where traditional and 5G mobile services share infrastructure, to improve service delivery and operational efficiency.

1. Zero-trust approach: A robust security posture from end to end, for all devices and software, will help reduce risk exposure across the 5G ecosystem. Having been assessed for their level of security before connecting to the network or resources, devices should only be allowed access to resources based on their need and security 'health.' Also, all software provisioning — from the core to the IoT device, and from firmware to the cloud — must be treated with a degree of scepticism, with resource hubs verified and code bases checked for malware prior to builds and deployments. Application programming interfaces (APIs) should be segmented and access controlled based on level of risk.

2. Universal encryption: To minimise the risk of data being compromised or corrupted, telecoms operators and other 5G participants should leverage strong encryption methods for securing the traffic between endpoints and services. This involves applying flexible methodologies that allow the encryption to be strengthened progressively over time as standards and risks evolve. Centralised key management processes will help mitigate 'man-in-the-middle' attacks, in which an attacker intervenes in a communication between two parties who believe they're communicating directly with each other.

3. Orchestration by AI: Machine learning (ML) and AI will have a vital role to play in identifying and mitigating ever-changing risks, providing the speed and accuracy of insight and intelligence needed to manage security policy across hyper-dense machine type communications and ultra-low latency applications. The capabilities of AI and ML technologies will see them used throughout the 5G architecture for security orchestration, including such activities as traffic analysis, deep packet inspection (DPI), threat identification and infection isolation.

AI: A powerful tool at the core of 5G networks, applications and devices

As telecoms operators embark on their 5G implementations, they are having to face up to unprecedented network complexity. The key elements driving this network complexity include the high-density distribution of 5G networks, the challenging configurations of large-scale antenna arrays, and infrastructure upgrades required across the network. Telcos will also need to prepare for the ongoing development of solutions to various needs — both predicted and un-predicted — that will emerge from IoT and related smart systems. This will demand an increasingly agile and responsive approach to network management.

AI will be critical in meeting these challenges by facilitating dynamic engagement with network quality, detecting and correcting network issues faster than is currently possible. AI will also be necessary for the full promise of network slicing to be realised; AI will enable operators to optimise their slicing strategies, responsively assessing, evaluating and determining slice allocations.

Looking beyond the network, recent [PwC thought leadership](#) has highlighted how the combination of AI and 5G will enable a new wave of connected devices that will redefine the word *smart* in two key respects. First, their user interfaces will be based not only on touch but increasingly also on voice working side-by-side with touch or even without it. Second, they will use discrete apps to trigger specific tasks requested by users and apply AI-driven algorithms to anticipate users' needs and meet them proactively.

Through these advances, AI and 5G will deliver a number of impacts for end users. One will be greater personalisation, as data transmitted over 5G fosters ever more automated and customized products and services. Another will be greater intimacy and humanity in people's digital experiences, as AI augments human capabilities and creates closer alliances between humans and machines. Together, these impacts will drive another: big increases in productivity and work/leisure bandwidth, with people freed up to pursue activities they're really interested in.

AI also has a role to play in cybersecurity in a 5G world. This is because AI and ML offer organisations powerful new tools to protect their systems from those with malicious intent — enabling them to combat the increasing sophistication of tools used by the attackers. In PwC's view, the most effective defence will involve using AI to sort through data and flag it for human analysis, with the human analysis feeding back into AI to improve its future predictions. This virtuous circle will provide the best defence for critical systems — creating a robust, secure basis for innovation to deliver the full benefits of 5G across all use cases.

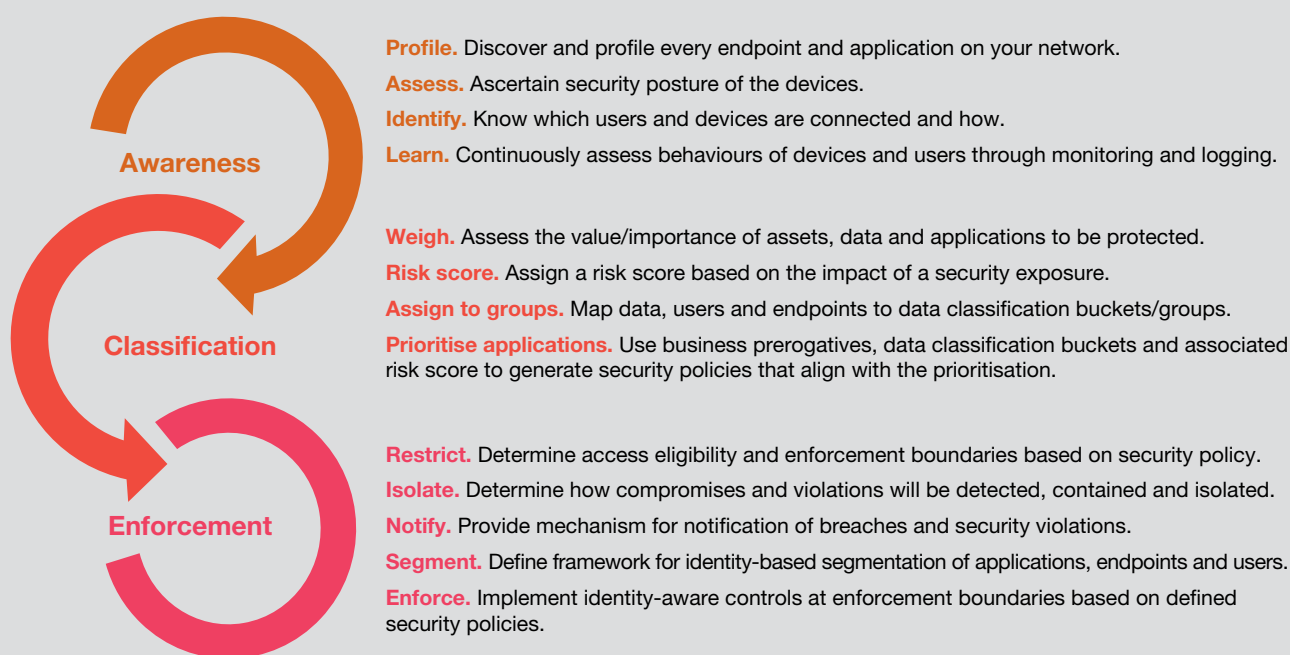
A vital first step towards protecting any network against cyber threats — 5G included — is to understand where vulnerabilities might arise.

Applied properly, the strategy will help organisations to work collectively to secure the 5G environment, while not overly impacting the ability of each business in the 5G ecosystem to serve its customers and interact with partners. A proven way of operationalising this strategy is to adopt an identity-driven model known as a zero-trust architecture (ZTA). This is a comprehensive information and infrastructure security model that addresses the 'who, what, where, why and how' when critical data and infrastructure assets are being accessed.

Under a ZTA, security capabilities are deployed to enforce policy and protect all users, devices, applications and data resources, and the communications traffic between them, regardless of location or connection method. The ACE model (awareness, classification, enforcement) depicted in Figure 1 can help companies to implement their ZTA.

Figure 1. Adopting a zero-trust philosophy for 5G

A comprehensive information and infrastructure security approach must address who, what, where, why and how critical data and infrastructure assets can be accessed. This identity-driven approach, commonly referred to as a zero-trust architecture (ZTA), deploys security capabilities to enforce policy and protect all users, devices, applications, data resources and the communications traffic between them regardless of location or connection method, using the ACE model.





Resilience by design

Companies that are supported by a zero-trust approach and its related architecture are well placed to build and embed cyber resilience in the 5G era. Valuable guidance on how to achieve this is available in PwC's latest [Digital Trust Insights report](#), which is based on survey data from more than 3,500 businesses worldwide.

The study finds firms that exhibit a high level of resiliency ranked in the top 25% in three areas related to developing resilience strategies. Fundamentally, their emphasis on 'resilience by design' puts this group far ahead of the rest. As a result, they are able to do the following:

- **Improve visibility of data assets.** Resilient companies consistently track how their data assets and existing processes are affecting the core of their business. The Digital Trust Insights report found that 91% of high-resilience companies maintain an accurate inventory of assets and refresh it on a rolling basis, compared with just 47% of the other respondents. It's critical that this inventory includes work with third parties, especially if the business works with a range of vendors — as it almost inevitably will in a 5G world.

Companies on the wrong side of the resilience divide can take action to catch up. By automating a real-time asset inventory and mapping the process for ongoing and accurate visibility across the network, organisations with low resilience can begin to address their vulnerabilities.

- **Test their tolerance.** Resilient companies look at the big picture and recognise their tolerance level for handling risky situations. We discovered that, when facing disruption to their critical business operations during a cyberattack, less than one-third of the enterprises in our study were able to defend themselves using impact tolerance, or the maximum impact to business services that a firm is prepared to tolerate in the wake of operational disruption. The other firms participating in our study — notably including the largest organisation surveyed — put their critical business services in jeopardy when such a disruption occurred.

By identifying critical business services, using metrics to define their impact tolerance, and then testing and mapping the impact tolerances to business services, companies can prepare to handle incoming threats.

- **Adapt and refine.** Resilient companies continuously evolve their business strategies. By improving the visibility of their data assets and testing their tolerance level, organisations put themselves in the high-resilience league. However, when facing the rapid development of technology, we found that only 34% of highly resilient companies adapt to the changes underway.

To ensure all-around protection, one-third of all highly resilient organisations refine their resiliency as they adopt new technologies. These firms often rely on a dedicated team to monitor the performance of core assets and IT dependencies, and can quickly and consistently redesign business services based on lessons learned from disruptions caused by cyber issues. As part of this preparedness, companies should adopt advanced threat-hunting capabilities that leverage automation and orchestration.

Together, these three characteristics enable an organisation to shift from a traditional disaster recovery/ business continuity model to resilience by design — which is something that many companies will need to do as they navigate the COVID-19 crisis recovery. Resilience by design is already proven to secure organisations, operations and systems against cyber threats — and is as relevant and effective in a 5G environment as in any other.

Companies on the wrong side of the resilience divide can take action to catch up. By automating a real-time asset inventory and mapping the process for ongoing and accurate visibility across the network, organisations with low resilience can begin to address their vulnerabilities.





Smart cities: Enabling the future of urban environments

With urban populations continuing to grow rapidly, putting increasing strains on traditional infrastructure, the race is on to transform existing cities around the world into smart cities. The British Standards Institute (BSI) defines a smart city as “the effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens.” This is a very apt definition, as it highlights how smart cities represent the marriage of physical and digital in the creation of cyber-physical systems (CPSs).

Digitisation can enhance a vast array of urban systems to meet citizens’ needs more effectively — most obviously in areas like transport and facilities management in buildings, but also in systems such as energy, water, public safety, waste management and pollution control. There is also potential to help manage public health emergencies, such as the coronavirus pandemic, by enabling modelling, detection, and prediction, and providing governments with real-time data to inform their decision-making process. 5G will help to realise the full potential of the smart-city concept by delivering an ultra-high-speed, low-latency platform to underpin these services.

Keeping smart-city systems secure will clearly be vital, both in terms of operating infrastructure and citizens’ personal data privacy. This can be achieved by ensuring all smart-city systems and connectivity are designed, assessed and conditioned from the ground up with security at their core, under a zero-trust approach.



Likely 5G use cases in Switzerland

Now let's zoom in on Switzerland. What path will 5G take in this country, and what will be the keys to its development?

To answer this question, we have to examine two more specific questions:

1. In this chapter we'll look at question of the most likely use cases for 5G given the specific structure of the economy in Switzerland
2. In the next chapter we'll look at the acceptance of new technology in Switzerland and how trust will affect it

What are the most likely 5G use cases in Switzerland?

Switzerland already has a very good mobile communication infrastructure in place: according to Swisscom, 5G coverage was already 90% by September 2020. This means the network infrastructure is ready for the first use cases.

In considering possible use cases, it's important to remember that Switzerland has no real large-scale manufacturing and heavy industry such as car making of its own. What it does have is smaller operations such as automotive suppliers that are part of complex global supply chains. There is plenty of manufacturing, but on a smaller scale or in areas such as pharma, high tech, medtech and precision engineering – which are in many cases heavily reliant on exports.

Another important factor is that Switzerland is a country that is poor in most natural resources but has a rich landscape of innovative niche players, trading companies and small enterprises.

Based on this brief sketch of the Swiss economy, we see the most promising use cases for 5G in areas such as:

- Industry automation and smart factories: Industrial Internet of Things (e.g. industries such as healthcare and logistics using 5G to interconnect sensors, actors and back-end applications)
- Supply chain and logistics (including production and delivery tracking, drones, etc.)
- Critical infrastructure (public transport, energy/power), including smart mobility solutions combining different transport solutions

Swiss use case in more detail: 5G in healthcare

5G in healthcare has the potential to fundamentally change medicine for the benefit of patients and society. 5G offers precisely the right capabilities for mission-critical services such as telemedicine and e-healthcare¹: speed, capacity, low latency, massive device interconnectivity and data-driven insights. Take latency, for example: compared with LTE, which has latencies of between 40 and 100 ms, delays of well below 10 ms are expected for 5G.

Wearables and the internet of medical things (IoMT) can transmit health data from patients to medical tracking systems in real time and can be used for remote patient monitoring. The technology will also allow patients to leave hospital earlier thanks to the availability of live home-monitoring options – something that's expected to reduce hospital costs by 16 percent over the next five years.² 5G will also make telemedicine (surgery via remote access) possible, enabling the patient to be admitted to the nearest hospital while having the benefit of the best available team all over Switzerland.

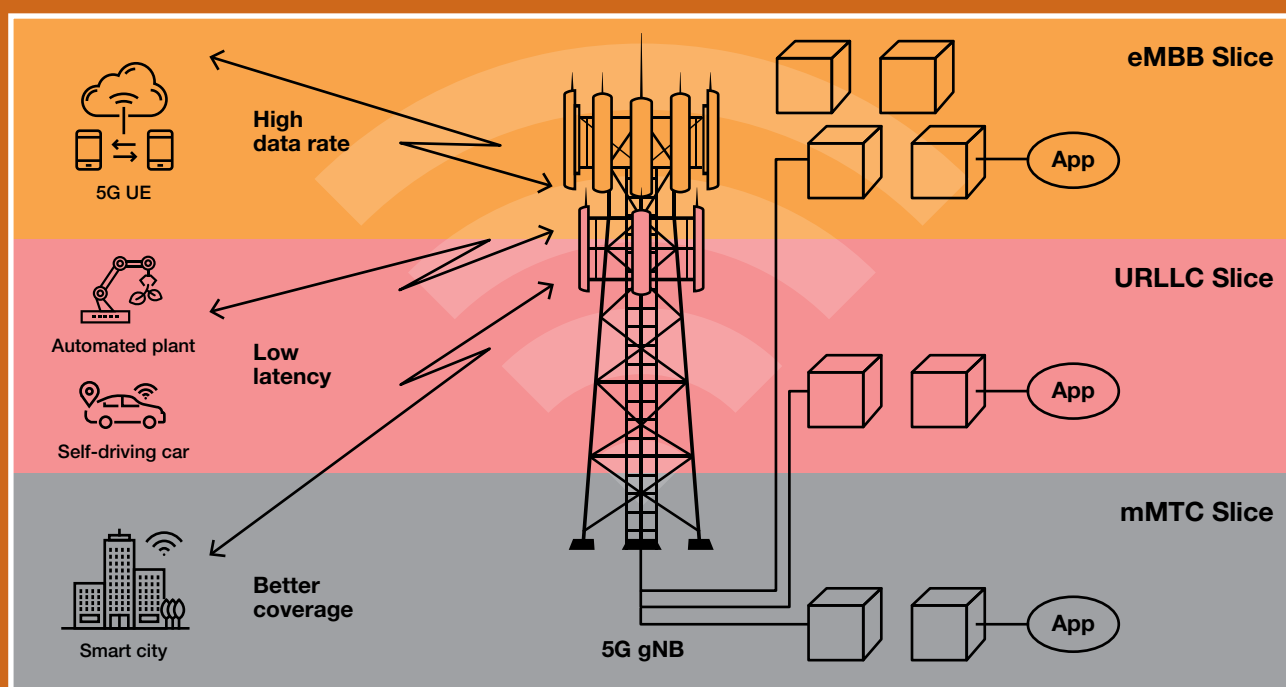
¹ <https://www.pwc.com/gx/en/tmt/5g/pwc-securing-5gs-future.pdf>, S. 5

² <https://www.swisscom.ch/de/magazin/neue-technologien/podcast-5g-im-gesundheitsbereich/>

What 5G technologies are we talking?

5G provides a new generation and design of network service to connect all kinds of devices with back-end applications.

- **Enhanced Mobile Broadband (eMBB):** eMBB aims to meet people's demand for an increasingly digital lifestyle, and focuses on services that have high bandwidth requirements such as high definition (HD) video, virtual reality (VR) and augmented reality (AR)
- **Ultra-reliable and Low-Latency Communications (uRLLC):** uRLLC aims to meet the demanding requirements of the digital industry and e-health, and focuses on latency-sensitive services such as assisted and automated driving, and remote management
- **Massive Machine Type Communications (mMTC):** mMTC aims to meet demands for a more highly developed digital society, and focuses on services such as smart city and smart agriculture with high requirements in terms of connection density. This includes small devices such as sensors and actors for smart cities and smart homes, and wearables with ultra-low costs and an integrated battery with a lifetime of 10 years and more.



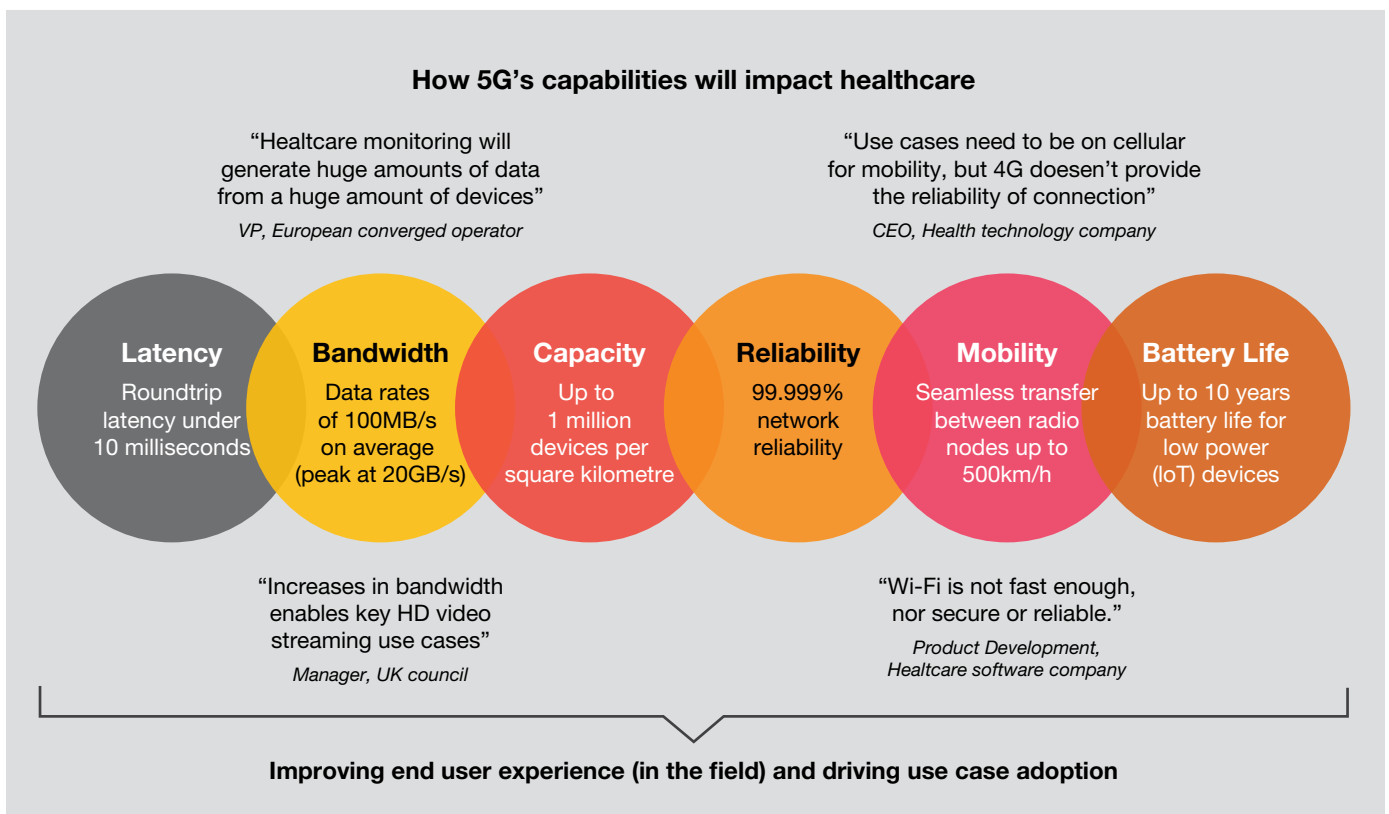
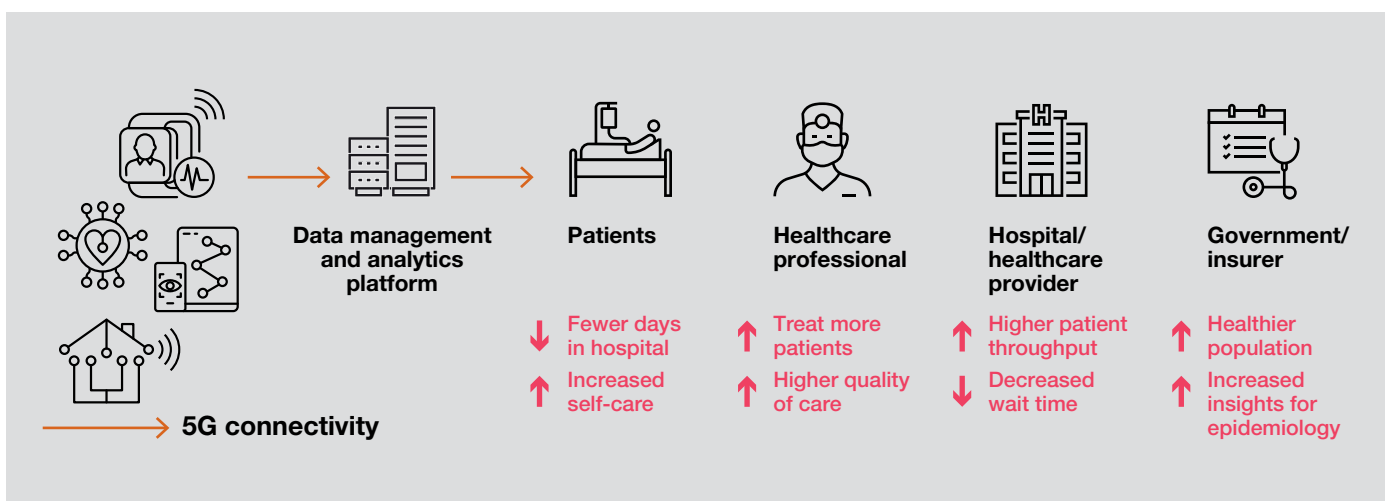
5G will also enable processes for tracking and tracing patients and equipment in hospitals to be optimised.³ According to a study by Market Research Future, the market for telemedicine is expected to grow 16.5 percent by 2023.⁴ Robotics will be able to perform medical interventions autonomously or semi-autonomously, and there will also be better use of artificial intelligence tools.⁵

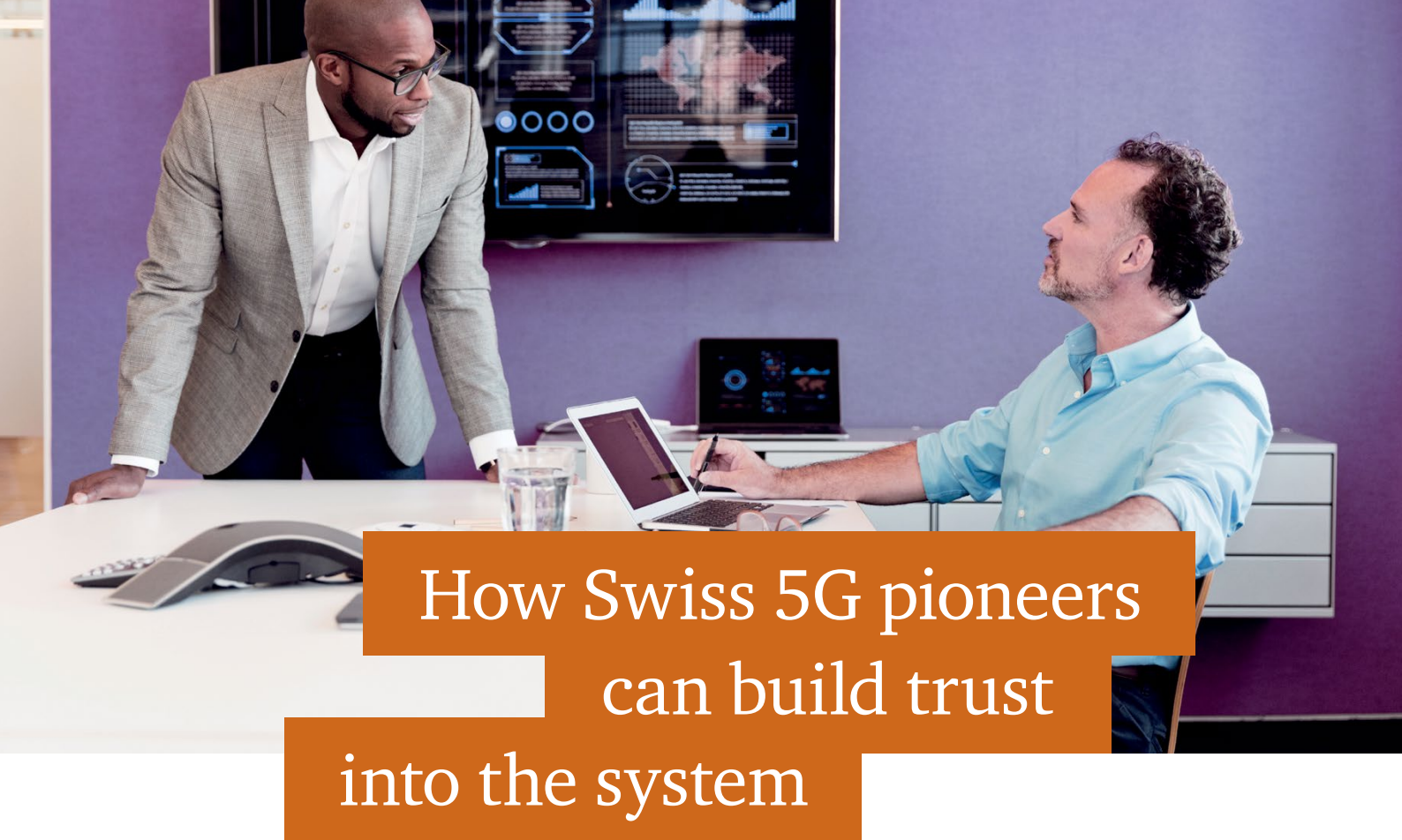
Despite all the benefits that 5G can bring to healthcare, it also introduces new security threat with potentially fatal consequences. In the next chapter we'll look at the crucial importance of trust if this use case is to get off the ground.

³ <https://healthtechmagazine.net/article/2020/02/what-expect-5g-healthcare>

⁴ <https://www.hhs.gov/sites/default/files/5g-security-for-healthcare.pdf>

⁵ <https://www.fiercehealthcare.com/tech/report-5g-has-potential-to-revolutionize-robotic-assisted-surgery-and-improve-availability>





How Swiss 5G pioneers can build trust into the system

Acceptance of new technology in Switzerland, and how trust will affect it

What's striking is that most of the likely use cases we've just described –including the healthcare case we described in more detail – involve processes that are very important to people, and situations where trust in the technology is crucial. It's a serious breach of trust if a drone is directed to the wrong destination because of a technical failure or if it's hacked and hijacked to deliver valuable goods such as drugs or medicine to the wrong address. It's just as serious if customer data is leaked or stolen, or if the geolocation or position data of the people involved is misused. Our healthcare use case involves the most serious threat of all: if a hacker succeeds in intercepting or blocking communications in telemedicine, people will die!

The EU-wide 5G cybersecurity risk assessment looked into these risks and found that the dependence of critical services on 5G networks means that a major disruption is likely to have serious consequences.⁶

Security risks associated with our use case for 5G in healthcare

In our healthcare use case we see how e-health produces and processes electronic data on patients their diseases and how they are treated. Such data is particularly sensitive if lost or stolen, and requires a high level of privacy. Not only this, but in healthcare high standards of integrity, availability and authenticity are needed to protect data from sensors or instructions to actors connected to the internet and prevent attackers from intercepting the connection. The growing number of devices being connected to networks makes it increasingly easy for hackers to find a weak link in the ecosystem. The more we rely on technology, the more we also have to consider the need for resilience to security threats.

The bottom line is that 5G, with its huge bandwidth and ultra-low latency, has the potential to enable new things and make the world a better place – but it also brings new threats of its own that will erode people's trust and enable criminals to extend their business if not anticipated and addressed sensitively, skilfully and from the outset. If the technology's not trustworthy, it puts the whole digital service innovation in question.

⁶ https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

How solid is Swiss people's basic trust in digital technology? While Switzerland frequently ranks as one of the most digital-friendly countries in the world, this is not the whole picture. According to some analyses⁷, Switzerland risks seeing its digital evolution stall if it doesn't keep up the momentum and proactively address important concerns. Despite almost universal acceptance of mobile devices, the installation of the 5G infrastructure in this country has already met with significant public resistance on health and safety grounds. Can you imagine how much greater this mistrust would be in the event of serious cybersecurity breaches in connection with 5G technology?

Cybersecurity is key

This brings us to the main point of our argument: if security is not considered from the outset, with trust built into the entire IT service, it will fail. With the advent of 5G, cybersecurity and communication security will become increasingly important. A zero-trust architecture is a good starting point. That's a pretty stark message, but we believe it's worth repeating: Trust is based on privacy and security. These aren't things you can add after a solution has been designed and built. They need to be included by design and by default. They need to be there from the start, and they need to protect the data over the entire life cycle, from end to end.

Security and trust applied to the healthcare use case

To build adequate security and trust into our healthcare use case example, it's important to adopt the type of holistic approach described earlier in this paper (Figure 1 on page 7) covering the three dimensions of awareness, classification and enforcement.⁸ To avoid the dangers inherent in the healthcare use case, it's important to consider all the endpoints involved and how security and trust will be established and maintained. To achieve state-of-the-art cybersecurity it's not sufficient to simply build a secure system with protective measures. You also need to continuously monitor and detect suspicious behaviour. After an anomaly has been detected, response and remediation actions have to follow. To do so, zero trust can be adapted to a 5G use case by addressing the following:

Awareness: Profile all endpoints involved and assess how trust can be established and security integrated by design. Devices and users need a unique identity that is assigned and can be verified reliably. Continuous monitoring and logging enables learning and detection of suspicious behaviour.

Classification: Weight the value and importance of each asset and the applications and data along the use case. A risk score helps when it comes to prioritising required protection measures for the desired trust level and formalising security policies.

Enforcement: Restrict access and enforce boundaries on the basis of the security policy. Use network segmentation and enforce policy on zone transitions. Provide mechanisms to notify relevant stakeholder in the event of a suspected or confirmed breach or policy violation.

With 5G digital businesses and collection of sensitive data will further evolve, since the way people work together will transform. At the same time threats will evolve as well.

That's why it is important to have risk based data protection and IT security measures in place from the onset for use cases processing sensitive data. Cyber resilience means to balance security measures for protection, detection, response and remediation with a target operation model tailored for each use case.

⁷ <https://digitalswitzerland.com/2019/10/11/swiss-digital-competitiveness-room-for-improvement-despite-good-ranking/>
<https://www.pidas.com/blog/en/rank-5-for-switzerland-in-the-international-digital-ranking-so-all-is-well>

⁸ <https://www.pwc.com/gx/en/tmt/5g/pwc-securing-5gs-future.pdf>

What can go wrong?

We can learn from the past and at least fix the issues we know lead to security breaches today:

- No reliable unique identifier to authenticate a device whenever a trusted channel needs to be established
- No way of updating security functions to remediate identified vulnerabilities
- Use of insecure cyphers to encrypt communication channels
- Failure to use mutual authentication when establishing a trusted channel to detect or avoid man-in-the-middle attacks and communication spoofing
- Unprotected storage of sensitive data (encryption of data is a good option to remedy this)
- When encryption is used, keys need to be truly random (not predictable or predefined), securely stored and transferred (key exchange) over the entire life cycle
- No back doors built in by the vendor or other interested parties
- Trust needs to be verified at each network boundary and between different providers

In the mMTC category of use cases, trust/security and ultra-low price often conflict, and security features end up being eroded for the sake of low cost. Since such devices are designed to work for 10 years or more, we need to take care that in areas where trust and security are required, the right level of security is integrated in the 5G technology enablement of low-cost devices, or that appropriate compensating controls are built into the 5G infrastructure itself.

The trust-related challenges of building a use case

As mentioned earlier, 5G is a game changer because multiple providers need to work together to build a use case. This brings a whole set of risks that need to be addressed. So how do you achieve trust and security in this situation? There are three parts to this answer.

- First, you have to understand and define security and trust at the overarching architecture level, supported with specific security concepts for all the relevant building blocks. Based on the data types transferred over 5G and processed in the ecosystem, different trust levels need to be considered. Given that trust requirements differ, there's no 'one-size-fits-all' approach.
- Second, you have to come up with and implement the architecture that will enable 5G solutions to work securely and reliably in the highly complex and potentially vulnerable environment where the use case aims to generate value.
- Third, you need to have a target operation model to maintain the trust level over the entire life cycle of the use case, the data stored and processed, and the providers involved.

As things stand at present, the weakest link is usually the human being using a device. For machine-to-machine communications, a main functionality of uRLLC and mMTC, the human factor can be eliminated – at least once it's been set up and configured. We should therefore be able to implement a good level of data protection and security if we really want to.

The three steps above break down into a whole series of concrete considerations when building 5G for a specific use case:

- The 5G network has to be built by the provider, and needs to fit all clients and use cases.
- The devices connected to the network need a reliable ID and security measures according to the desired trust level.
- For use cases requiring an enhanced trust level, network slicing⁹ should be used to create a virtual private network and to formally enrol devices before they're enabled for a specific use case.
- Device and user identity, and authentication and management, need to be assigned to a provider with defined security policies and a mechanism to enforce them.
- Edge computing is the first enforcement point where devices and users need to be verified before data can be accessed and processed.
- Back-end data processing and data storage have to have the same trust level to enable data processing and ensure that data access is secure and privacy is enforced.

⁹ "Network slicing" is a 5G feature to create software defined virtual private networks over 5G


A photograph of a modern office environment. In the foreground, a man in a dark blue shirt and dark trousers stands with his back to the camera, looking towards a group of people. Two women are seated at a white table; one is looking at a laptop, and the other is looking towards the man standing. The office has glass partitions, and the lighting is warm and modern.

How do you make sure it goes right?

Most parties involved agree that 5G is the next big thing and a key component of self-driving cars, e-health, smart farming and IIoT. So it's already clear that a trustworthy network is required. Unlike the internet, which was built without trust in mind (and failed to remedy this shortcoming later on), we should aim to build at least one segment of 5G as trustworthy network. I don't need a high level of trust to watch movies on my tablet. But if my insulin pump or pacemaker has no trusted channel to the monitoring centre, I'm in deep trouble. The same goes for self-driving cars, drones and trucks.

To sum up: end-to-end security, privacy and trust are crucial

5G technology, used properly, can potentially make a great difference to the relevance of the Swiss economy and people's lives – but only if they trust it. For 5G solutions to work, end-to-end security, privacy and trust must be built into the system from the very outset.



Conclusion: Seize the 5G moment through trust, resilience and enablement

It is often claimed that 5G will transform the world, but it's important not to get swept away in the hype. Although the world is clearly changing, what's really driving that change is the near-universal availability of smart connected devices. The network through which those devices connect is just one part of this new environment, albeit an important one.

That said, there's no doubt that the advent of 5G represents a shift in the cybersecurity landscape. It will be the medium through which the workflow and decision chains of the automated interconnected components in tomorrow's critical industrial and societal networks will flow. And without 5G, the growing millions of connected devices — especially those involved in applications such as self-driving cars, where low latency and connectivity at high speeds are prerequisites — would be effectively useless. 5G is certainly not overhyped in terms of being the 'connected' component of many smart connected devices.

Against this background, nobody would question that effective cybersecurity across the 5G ecosystem is non-negotiable. However, it's important to note that many of the security vulnerabilities commonly laid at 5G's door are not actually specific to the 5G technology itself. If devices, encryption algorithms or AI engines connected to 5G networks are penetrated or compromised, it's a problem for 5G operators and users. But it's not specifically a 5G problem. Effective security in a 5G world requires every participant in the value chain to play their part. That's why we propose a zero-trust approach backed up by 'resilience by design' — putting cybersecurity at the centre of every 5G deployment where sensitive data is processed.

To do this, company leaders will need to focus on three fundamental pillars of security: **trust**, to drive adoption of cybersecurity measures; **resilience**, to prevent, ride out and recover from disruptive attacks; and **enablement**, to move fast to overcome new and existing threats. These pillars are the foundation of a sound cyber strategy and will ensure that companies can roll out 5G quickly and safely, enabling individuals, business and society as a whole to enjoy the potential of this powerful new tool confidently and securely.



Contacts

To find out more about how PwC can support your journey to a 5G-enabled future, please contact us.

Technology, Media and Telecommunications

Wilson Chow

Partner, Global Technology, Media and Telecommunications Leader, PwC China
+86 755 8261 8886
wilson.wy.chow@cn.pwc.com

Kirolous Zikry

Senior Manager, PwC UK
+44 77 2563 3388
kirolous.s.zikry@pwc.com

PwC Global – Cybersecurity und Privacy

Richard Horne

Partner, Lead Cybersecurity and Privacy, PwC UK
+44 77 7555 3373
richard.horne@pwc.com

Marin Ivezic

Partner, Industrial and IoT Cybersecurity, PwC Canada
+1 416 687 8672
m.ivezic@pwc.com

Peter Durojaiye

Director, EMEA Cyber Impact Center, PwC Hungary
+36 70 685 0360
peter.a.durojaiye@pwc.com

Grant Waterfall

Partner, EMEA Cybersecurity and Privacy Leader, PwC UK
+44 77 1144 5396
grant.r.waterfall@pwc.com

PwC Switzerland – Cybersecurity und Privacy

Urs Küderli

Partner, Lead Cybersecurity and Privacy, PwC Switzerland
+41 58 792 42 21
urs.kuederli@pwc.ch

Yan Borboën

Partner, Cybersecurity and Privacy, PwC Switzerland
+41 58 792 84 59
yan.borboen@pwc.ch

Lorenz Neher

Senior Manager, Head Security Architecture and Operation, PwC Switzerland
+41 58 792 47 85
lorenz.neher@pwc.ch

www.pwc.ch/cybersecurity

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com