Designing the future,

how we work, live and thrive in a secure interconnected society and realizing the benefits of 5G

Executive summary

The future of the internet is wireless and we live in a society where time is measured by how quickly a transaction can be made. But 'what is a transaction?', you may ask. Well, consider how many times you have done a Google search for: food, clothing or locations - and these are just three of the most frequently searched terms.

In an industry of connected devices – services, speed, convenience and availability are all critical aspects. The global Covid-19 pandemic has accelerated the adoption of an always-on service economy. As a result, many businesses were forced to innovate quickly and to accelerate their transformation and many now seek to set themselves apart through the use of technology as a differentiator.

Contents

The market drivers 03

Enabling a secure and connected society 04

‘5G in mobility, healthcare, manufacturing, and retail, the use cases we identified in these **four commercial domains alone could boost global GDP by $1.2 trillion to $2 trillion by 2030’.**

(McKinsey, February 20, 2020 | Discussion Paper)

The internet enabled access to information and 5G can be seen as a bridge to the digital world, to further enhance accessibility and to use data to make informed decisions. The endless number of connected devices out there has fueled an insatiable desire for data and the ability to deliver ubiquitous, fast, efficient and effective access is now commonplace.

More and more services are going to be delivered and consumed using 5G. In the meantime, conversations surrounding integrity is high on the agenda of all stakeholders and we share context that needs to be given to the security of connected things and the impact of 5G.

Is security inherent? Does security stop at the device location? How will we manage the threats associated with billions of devices? The industry is already talking about increased cyberattacks with the wide adoption of cloud and Software as a Service (SaaS) and there is a need for new security measures to stay ahead of threats.

The 2021 Olympics highlighted the need for an always-on event because the pandemic prevented in-person attendance or limited attendance to a minimum number of in-person spectators. Broadcasters relied on the internet and 5G to have people connected. NTT understands how to enable and secure a connected future by leveraging the benefits of 5G technology.

At NTT, we believe in enabling a secure and interconnected future, and in actively helping industries take advantage of this ‘interconnectedness’. Our heritage is built on connectivity and today, we serve the world’s most used internet applications through our global network and our Data Centers. Most importantly, we realize the need for continuous monitoring of the integrity of these applications. There’s where our AI and machine learning can help ensure the safety and security of these applications.

The market drivers

By 2025, the 5G market is expected to be valued in the trillions of dollars. The ongoing effects from the pandemic will continue, driving businesses to modernize and to transform. It ranges from how students will be required to tap into reliable internet connectivity at school, to how consumers now interact with digital services, such as those in the healthcare sector.

The desire for people and systems to coexist will benefit all industries and not be limited to any single organization with the best infrastructure.

New business models and economic growth will come through all industries, including developing economies. We will continue to see new e-service models created through new partnerships. Real-time supply chain management is now feasible and 5G is expected to further drive the consumption and effective supply of the right products, while limiting waste.

‘Who will benefit?’ is often the rebuttal and at what cost will these benefits be realized? Markets in developed countries have benefitted from the internet and some of the most popular companies in the world today exist because of the internet.

The value for all is in the data and how devices, applications and infrastructure will enable continued and sustainable economic growth best using data and interconnectedness.

In particular, industries such as healthcare (telemedicine), manufacturing (smart factories) and transportation (infrastructure and autonomous cars) will benefit from 5G. But with that, also comes the increased risk of device sprawl and new vulnerabilities, ransomware and other threats. The transformation and introduction of 5G allows enterprises to deliver better services but will inevitably introduce new threats as both macro and micro factors bring increased security risks.

The world has already seen all three industries above experience various types of security breaches. Going forward, as 5G accelerates access and connectivity, these industries will need to look into enhancing security measures in order to ensure their integrity and resilience.

1. **Secure the device**
   Questions to ask include: What kind of security is currently built into the device? And what additional security layers could be put in place to ensure that you are enabling a secure environment that meets corporate standards, while mitigating known threats?

2. **Secure the perimeter**
   The ‘perimeter’, as we know it, has shifted and concepts surrounding data being the perimeter or the user being the perimeter have been further elevated with the ‘speed’ of access. Security should then be based on active threats, and not just risks because we’ve seen an increase in ransomware, as well as evidence of extortion in 2021. Privacy, personalization and reliability needs to be a core focus.

3. **Secure the application**
   Applications have enabled business transformation as more and more organizations embrace technologies to modernize the way they engage new markets. The pandemic has accelerated the coverage and access to these applications, due to new demand for always-on services. The demand for greater personalization and data makes the need for these applications even greater.

Enabling a secure and connected society

5G is said to enable better security. However, security is viewed differently across industries, countries and governments. As such, adequate thought and consideration must be given to how data is consumed, where data will reside, and the regulations that need to be in place to govern the use of data.

1. **Devices**
   The scale of mobility, where mobile devices have become micro platforms – we can now work from anywhere, and have access to information to make important decisions from wherever we are. Soon, speed will no longer be an inhibitor in any market. Embedded sensors will be implemented in all things mobile and the ability to realize the value of 'automation' (eg. autonomous vehicles) will benefit from this speed. However, in these industries, to realize the benefit we must first ensure security. An autonomous car will have so many connected components, all to help make decisions and ultimately to ensure efficiency of a self-driving car. Security is critical to ensure integrity of its software and connectivity to enable this autonomous vehicle to serve its function securely.
2. **Networks**
   Scale, coverage, consistency, and cost effectiveness are all intrinsic benefits from 5G. 5G is designed to deliver peak data rates of up to 20 Gbps based on IMT-2020 requirements. 5G is designed to provide much more network capacity and is fast becoming an extension of enterprise networks. Enterprise IT has seen an evolution of private networks to shared MPLS networks, and now SDWAN and SASE. All inherently have network providers implementing a level of security and quality of service. Enterprises are grappling with the need to implement a zero-trust architecture, which sees the enforcement of the least privileged. Focus on 5G will be on segmentation and security will be up to the edge.
3. **Applications**
   The cloud enabled the fast deployment of applications and encouraged businesses to engage their users to drive customer personalization and customization. The deployment of 5G has created the ability to enable connecting more devices than ever before. There are now applications for ordering food (personalization), hailing a ride (privacy) and making payments (reliability), but this requires a stronger focus on the resilience of both static and dynamic applications. We have seen lots of news in 2021 from large retailers who have had applications compromised with the loss of 'potential' revenue, as well as healthcare providers who have had healthcare devices compromised with published vulnerabilities.

How industry and enterprises deal with this is critical, as the security industry is grappling with a macro trend of shortage of skilled resources. NTT has invested in:

Realizing the benefits

5G offers value to business, users and society as a whole. The realization of smart cities, smart factories and Industry 4.0 in general will create new jobs, increase economic prosperity and improve productivity. In order to maintain integrity, 'continuous monitoring' of the ability to detect and respond to known threats is a key business enabler. The attack surface is already vast and if 5G is to bring the benefits described, this surface will be greater than our ability to control it without machine learning and automation. NTT has invested in a security platform that allows clients, regardless of industry, vertical or country to maintain visibility of all known threats that targets a client's digital footprint.

Assurance

Enterprises and industries need to continuously validate the security inherent in the connected devices and the 5G infrastructure to run their services. In addition, enterprises need to extend visibility to their attack surface and validate what known threats exist, and continuously monitor for new, emerging threats. Traditional testing may not be adequate, and the use the of automated tools like breach and attack simulation with playbooks to run continuous assessment should be considered with the broader footprint and attack surface to manage security, compliance and risk.

Vulnerability Management

The last year has highlighted how much more diligence companies globally would require in the new world order. The market has also seen some new entrants that help address assets inventory. There's also been a few unicorns created with the increased adoption of the cloud. The industry labels these as: application scanning, software and asset management. Meanwhile, OT , IoT , is now the focus and raises concerns with supply chains for a number of reasons – eg. Manufacturing, age of infrastructure, location, environments and change windows. Our approach is that companies should apply a concerted effort. Because of the process and legitimacy of some suppliers, companies need to build maturity and take a risk and a best practice-based approach to manage new threats.

Incident response

Industries in general, have prioritized responding to incidents following much publicized incidents across the globe that have not only disrupted critical infrastructure and manufacturing, but also highlighted the lack of skilled resources to help respond effectively. This has also been accelerated with the move and pace the world is now taking to connect everything.


NTT