IOT ~ THE INTERNET OF TRANSFORMATION 2020

Whitepaper

JUNIPER RESEARCH

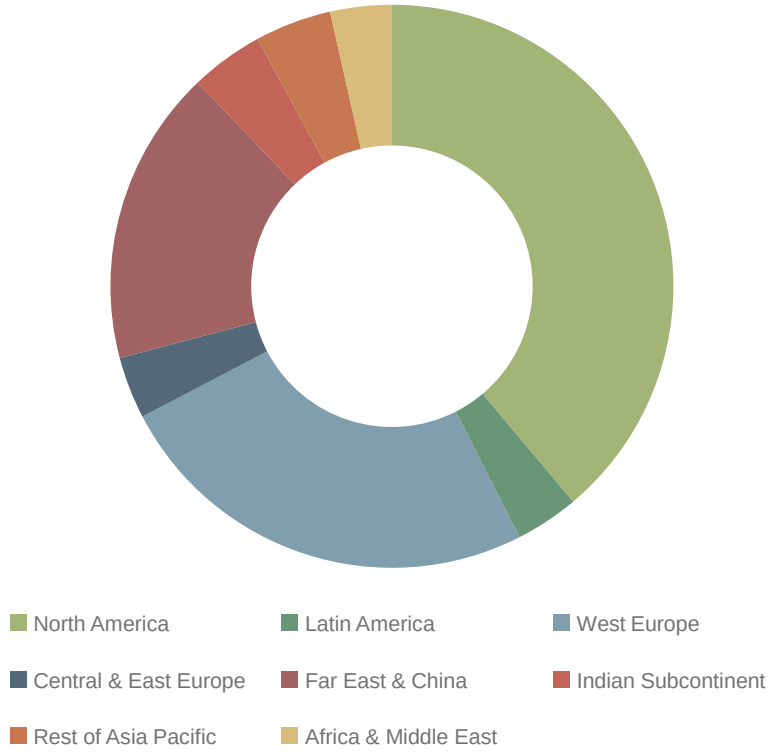
1.1 Introduction to the IoT

The IoT (Internet of Things) has made its way into the mainstream consciousness by virtue of the media and a selected number of innovative consumer devices. Similar to many other modern developments, like digitisation, smart, AI, design thinking, disruption or innovation, the Internet of Things has become yet another buzzword.

In the past, the Internet has been used as a communications network for which data has mostly been generated manually by humans. Due to developments in radio technology and falling component costs, the Internet is now also being used as a communications network for machines to communicate with each other and/or directly with humans.

Juniper Research has identified private cellular networks as a key driver of growth of IoT adoption over the next five years. This trend has been slowly establishing itself as LTE networks can be leveraged to do so, offering a wireless data connection. With 5G having launched, Juniper Research anticipates that the wireless standards will serve to accelerate the adoption of private cellular networks over the next five years.

Figure 1: Global Number of Connected IoT Units (m), Split by 8 Key Regions in 2019: 35.7 billion



Source: Juniper Research

Next to the many different definitions, Juniper Research offers two quite distinct variants, a simple one as a basic introduction to IoT and a holistic one representing the complexity of IoT solutions many companies must face in reality:

IoT is the interconnection of 'things' (or 'devices': a combination of hard- and software) via a network infrastructure including systems that store and process data, as well as some sort of user interface to understand and react (manually or automatically) on the collected data.

Such a definition of IoT typically includes the following technological elements:

- **Device hardware** – acting as the interface between the real and digital world, typically including sensors, embedded computers and physical network infrastructure.
- **Device software** – OS for embedded computers and edge applications on top of the OS, offering possibilities like data acquisition, streaming to the cloud, data structuring and filtering, local analytics, etc.
- **Communications** – protocols, eg Wi-Fi, WAN, LAN, NB-IoT (Narrow Band-IoT), Bluetooth, etc, being used by network infrastructures to enable the devices to exchange information with the rest of the world; the cloud or third-party devices.
- **Cloud platform** – data collection, processing, management and analysis.
- **Cloud applications** – end-user applications being web-based, on desktop, mobile phones, or on wearables.

The important difference to the simpler definition is that this holistic one includes several of the elements that might eventually make or break the final solution. Adaptability, standards, unique identification, interfaces and security are just some of the important words the reader might want to remember and reflect on, to understand the details of IoT that might lead to success or failure.

1.2 Market Challenges & Strategic Recommendations

Although the IoT has grown immensely throughout the last decade, solution providers still face a multitude of challenges when trying to achieve a successful development, implementation and deployment of IoT technologies.

The biggest problem of all is the variety of complexities IoT brings to the table. First and foremost, companies need to identify a solid user problem that demands a smarter solution than those being offered on the market so far.

Secondly, the IoT solution's design needs to enable scalability, security, interoperability and the ability for future maintenance, as well as future adaptability to potential new sensors and unexpected human use behaviours.

Thirdly, solution providers need to implement IoT systems in existing infrastructure and integrate software accordingly, which is often not easy.

Fourthly, companies need to continuously monitor security issues and ideally also include proactive security measures throughout the entire value chain. Finally, (certainly this list is not comprehensive) companies

need to ensure their IoT business cases are viable and sustainable in the long run. To offer a more comprehensive overview of this complexity Juniper Research has identified the following topical clusters for challenges and strategies:

- **Solving a problem & providing real value**
- **Ensuring cybersecurity & data privacy**
- **Interoperability, fragmentation & standardisation**
- **Implementation**
- **Organisational expertise & culture**
- **Sustainability**

1.2.1 Solving a Problem & Providing Real Value

According to multiple high-end managers in the IoT industry, the primary reason why companies did not make it beyond the Proof of Concept stage, was that the business case was simply too weak, not having identified a unique user problem that was worth solving or providing real value with the planned IoT future product.

1.2.2 Ensuring Cybersecurity & Data Privacy

Nearly all the interviewed experts from the industry, as well as any article on IoT challenges, point out that cybersecurity and data privacy are issues that have not yet been resolved anywhere in the community. It is probably the most important technology challenge, while also being arguably unsolvable. While it is certainly not an awareness problem, it is an ongoing race between cybercriminals developing new forms of attacks and defenders creating new forms of detections. In addition to this 'classic' problem of cybersecurity, IoT security demands solutions that protect the network layer, the hardware layer and the cloud software. This makes it even more complex, as it requires a system of well-connected and seamless functioning security solutions and providers.

The investment to improve cybersecurity has increased heavily over the past few years but so has the number of breaches of connected devices. Looking at the SonicWall's Cyber Threat Report 2020, however, it detected only a 'moderate 5% increase in IoT malware, with total volume reaching 34.3 million attacks', which is not too bad compared to the 2018 report which measured a 217% increase compared to 2017. Other statistics from F-Secure, however, detected a 300% increase of attack traffic with more than 2.9 billion events in H1 2019, with most attacks on the Telnet protocol (760 million), followed by the UPnP protocol (611 million).

i. IoT – The New Surface for Cyberattacks

The dramatic increase in connected devices revealed an attack surface that cybercriminals have never been seen before. The challenges associated with defending data security and privacy will only increase with time as the deployment of connected devices constantly accelerates.

ii. Old Industrial Systems at Risk

Many rather old industrial systems get indirectly connected to the Internet and therefore to the IoT. The fact that many units have been installed for decades means that strong security was never considered. Many units are therefore potentially vulnerable to attacks which could lead to catastrophic, even life-threatening, harm.

iii. Missing In-house Competencies

Many enterprises enter the IoT market without any previous connectivity or cybersecurity in-house competency. For them the issue will be about costs as well as implementation. Eschewing a managed security solution may well be more cost effective, but carry a higher risk and a potentially higher financial impact later on.

iv. Low Margins for IoT Devices & Continuous Device Access

The consumer IoT market is composed of a very wide range of hardware vendors, from large corporates to crowdfunded start-ups. Therefore, competition in the market is extremely high, while margins are typically low. The effect is that no single vendor, outside global corporates such as Google, Apple and Samsung, enjoy the benefits of economy of scale in the context of consumer IoT and therefore lack essential security funding. The fact that the hardware is software-enabled is an additional challenge. It requires ongoing support, so the relationship between the vendor and the end-user is no longer transactional, but veers to service-orientated. In a situation where margins are already low, the additional costs required to develop and maintain security solutions for products has been shown to be untenable.

The issue is magnified as there are a large number of white-label products on the market, where it is difficult to identify the ODM (Original Design Manufacturer). Even where this is possible, they may not be in a position to issue a software patch to address any security issues. The net effect is that poor security in this segment impacts the wider IoT; Dyn is a clear example of this. It also emphasises the critical nature of robust defences to mitigate the risks from weak links in the chain.

1.2.3 Interoperability, Fragmentation & Standardisation

Fragmentation has always been a problem for the IoT. As IoT solutions can, and do, use different wireless network protocols like Wi-Fi, LoRa, Zigbee, Bluetooth or 5G, shows the fragmentation at a very basic level. Each of these network types has specific characteristics optimised for different use cases, which poses the risk for significant financial and time costs for connecting solutions from different communication protocols.

In the field of the smart home and digital healthcare, fragmentation is especially problematic. For smart home devices, it means the risk of individual gadgets or appliances not being able to interoperate, which can have negative effects on the ease of use for end-users. In healthcare, a well-known fragmentation example is EHR (Electronic Health Records). The single biggest hurdle to the benefits offered by EHR adoption was, and is, interoperability. While many healthcare providers are adopting EHRs, these are systems that hold the data generated in an isolated, restricted way, with data access being restricted to that single system. This makes it difficult for any third-party system to interface with the EHR.

Ultimately, legislative frameworks also experience issues with fragmentation. In Europe alone there is the NIS Directive (the Directive on Security of Network and Information Systems), ENISA (the European Cybersecurity Act), NLF (the New Legislative Framework), the Radio Equipment Directive, the Machinery Directive, and the Low Voltage Directive. These all have to work together and be aligned for the complexity of IoT system being built today. This legislative landscape exposes the industry to a set of patchy and unaligned laws, which create inconsistent and overlapping requirements and technical standards.

1.3 IoT Movers & Shakers

Scott Guthrie

Microsoft

EVP Cloud & AI Group

As EVP of the Microsoft Cloud + AI Group, Scott Guthrie is responsible for the company's computing fabric (cloud and edge, including cloud infrastructure, server, database, CRM, ERP, management) and AI platform (infrastructure, runtimes, frameworks, tools and higher-level services around perception, knowledge and cognition).

Prior to leading the Cloud + AI Group, Guthrie helped lead Microsoft Azure, Microsoft's public cloud platform. Since joining the company in 1997, he has made critical contributions to many of Microsoft's key cloud, server and development technologies. He was one of the original founders of the .NET project.

Guthrie graduated with a bachelor's degree in computer science from Duke University.

Scott Barkley

Cisco Jasper

Head of IoT Cloud Product Management

Scott Barkley has led the IoT Cloud Product Management team at Cisco Jasper since 2005.

Previously, he spent several years in product, marketing and sales leadership positions at Siebel Systems. Before this, he was in Business Development and Operations roles for several software and financial organisations.

Barkley has a BA from Princeton University and an MBA from the Kellogg Graduate School of Business, where he was a Wade Fetzer Scholar.

Bhaskar Gorti

Nokia

President, Nokia Software & Chief Digital Officer

Bhaskar Gorti oversaw Alcatel-Lucent's business units that developed technologies for cloud-based networking and virtualisation, These include NFV, as well as Communications and Collaborations suites, OSS, Charging/Policy/Payments portfolio, Customer Experience Management, Network Performance and Intelligence, and the Cyber-Security monitoring and prevention software platforms.

Previously, Gorti was Senior Vice-President and General Manager of Oracle Communications Global Business Unit. He had been with Portal Software since 2002 and led the sale to Oracle in 2006 to form the Communications business at Oracle.

Carsten Ahrens

G+D

CEO of G+D Mobile Security

Carsten Ahrens is the CEO of Giesecke+Devrient Mobile Security GmbH. As well as his duties as CEO, he is responsible for the areas of Strategy, Compliance, Sales, Divisions, Marketing and Communications, and the Technology Office. Moreover, he is currently temporarily in charge of Research and Development, Personnel, Operations, and Professional Services.

Ahrens has been working in the Mobile Security unit at G+D since 2013, initially as the Manager of the Telecommunication Industries division and later as the Chief Sales and Marketing Officer. He held various management positions before joining G+D, including CTO/COO at Funkwerk AG and Managing Director at Ericsson GmbH.

Romil Bahl

KORE

President and CEO

Romil Bahl is the CEO of KORE, an IoT specialist based in the US. He has almost 30 years of experience in the Information Technology, Consulting and Professional Services arenas.

Prior to KORE, Bahl was President and CEO of Lochbridge, a technology solutions provider in the IoT, Connected Car and Digital Enablement space.

He was EVP and GM of Global Industries for CSC, expanding its operations in cloud, cybersecurity and Big Data.

Bahl has had leadership roles at AT Kearney, Infosys and Deloitte. He has an MBA from the University of Texas, Austin and a Bachelor of Engineering degree from the Directorate of Marine Engineering & Technology in Kolkata, India.

Gregory Gundelfinger

Telna

CEO

Gregory Gundelfinger has been the CEO of Telna since July 2016. A lawyer by profession and a serial entrepreneur from South Africa, he started and sold several successful companies.

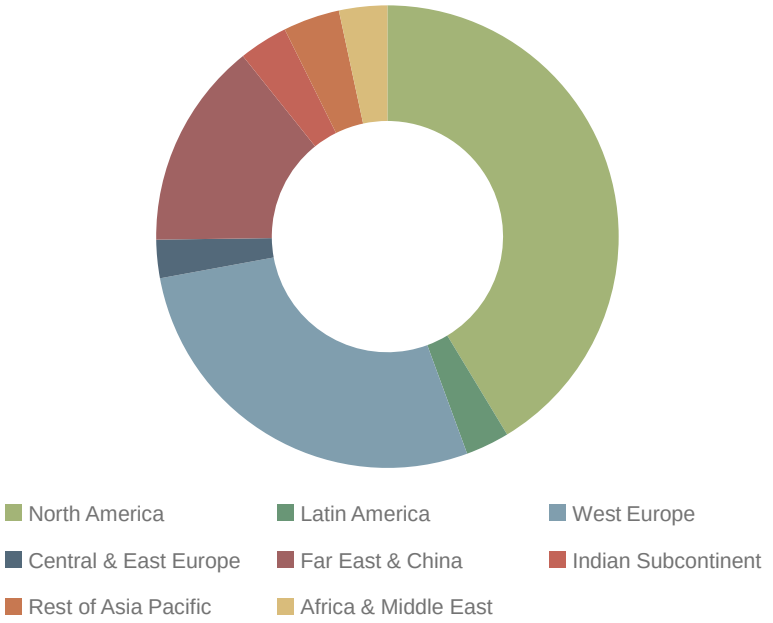
Gundelfinger relocated to North America to pursue a business in technology. He identified that eSIM, converged communication and software-defined networks were the future of cellular communications. He led the acquisition of Telna in 2015 and developed himself into a thought-leader for telecommunications. Gundelfinger is now a sought-after speaker at annual eSIM summits, MVNO and IoT conferences in both Europe and the Americas.

He has a Bachelor of Law degree from the University of South Africa.

1.4 Market Summary: Total Connected IoT Units

The total number of IoT connections will reach 83 billion by 2024, rising from 35 billion connections in 2020; a growth of 130% over the next four years. The industrial sector has been identified as a key driver of this growth. Expansion will be driven by the increasing use of private networks that leverage cellular networks standards.

Figure 2: Total Connected IoT Units, Split by 8 Key Regions in 2024: 83 billion



Source: Juniper Research

- The industrial sector, including manufacturing, retail and agriculture, will account for over 70% of all IoT connections by 2024. The emergence of cost-efficient private cellular networks would be a key driver of growth over the next 4 years, and recent increases in demand for private LTE networks will carry forward to private 5G networks as the cost of the technology falls over the next two years.
- The number of industrial IoT units in service will grow 180% over the next four years.
- The increasing complexity of private IoT networks will mean that platforms must implement steps to maximise security in all layers of the IoT ecosystem, including devices, connectivity and the platform itself.
- Vendors must implement security procedures that are highly scalable and can cope as network architectures become increasingly complex. Juniper Research suggests two key areas of focus; the use of network segmentation to mitigate the risks of lateral movement cybersecurity attacks and ensuring that the lifecycle management of network assets is properly maintained.

Order the Full Research

Internet of Things' latest research provides critical insight into the fast-moving world of the IoT featuring technology impact analysis split by consumer, industrial and public sectors. Analysing challenges, impact and opportunities on a segment-by-segment basis in tandem with overarching strategic approaches, the incisive study provides in-depth analysis of the future outlook for the IoT in terms of business models and service provider opportunities, as well as key market forces that are impacting the area.

Key Features

- **IoT Core Strategy Analysis:** Includes current and future strategies, challenges and approaches for Cybersecurity and Data Privacy; Identity Management; IoT Implementation; Interoperability, Fragmentation and Standardisation; Privacy.
- **Sector Dynamics:** Analyses the impact of IoT vertical markets for the consumer, industrial and public service segments, aligned with a breakdown of current market trends. The analysis is split by Consumer IoT, Industrial IoT and Public IoT.
- **Juniper Research Leaderboard:** 12 IoT solution vendors compared, scored and positioned on the Juniper Research Leaderboard matrix, including Cisco, IBM and Oracle.
- **Benchmark Industry Forecasts:** Market segment forecasts for IoT adoption for the consumer, industrial and public services segments, including unit installed base, unit shipments, hardware revenue, and software platform revenue.

http://www.juniperresearch.com

What's in this Research?

1. **Deep Dive Strategy & Competition** – Strategic analysis of market dynamics, drivers and trends, together with a detailed investigation of established and emerging IoT technologies (PDF)
2. **Deep Dive Data & Forecasting** – IoT market prospects analysis, together with 5 year forecasts for vital IoT metrics across 8 key vertical use cases (PDF)
3. **Interactive Forecast Excel** – Highly granular dataset comprising more than 17,000 datapoints, allied to an Interactive Scenario tool giving users the ability to manipulate Juniper Research's data (Interactive XL).
4. harvest Online Data Platform: 12 months' access to all of the data in our online data platform, including continuous data updates and exportable charts, tables and graphs (Online).

Publications Details

Publication date: April 2020

Authors: Markus Rothmuller and Sam Barker

Contact: For more information contact info@juniperresearch.com

Juniper Research Ltd, 9 Cedarwood, Chineham Park, Basingstoke, Hampshire, RG24 8WD UK

Tel: UK: +44 (0)1256 830002/475656 USA: +1 408 716 5483 (International answering service)