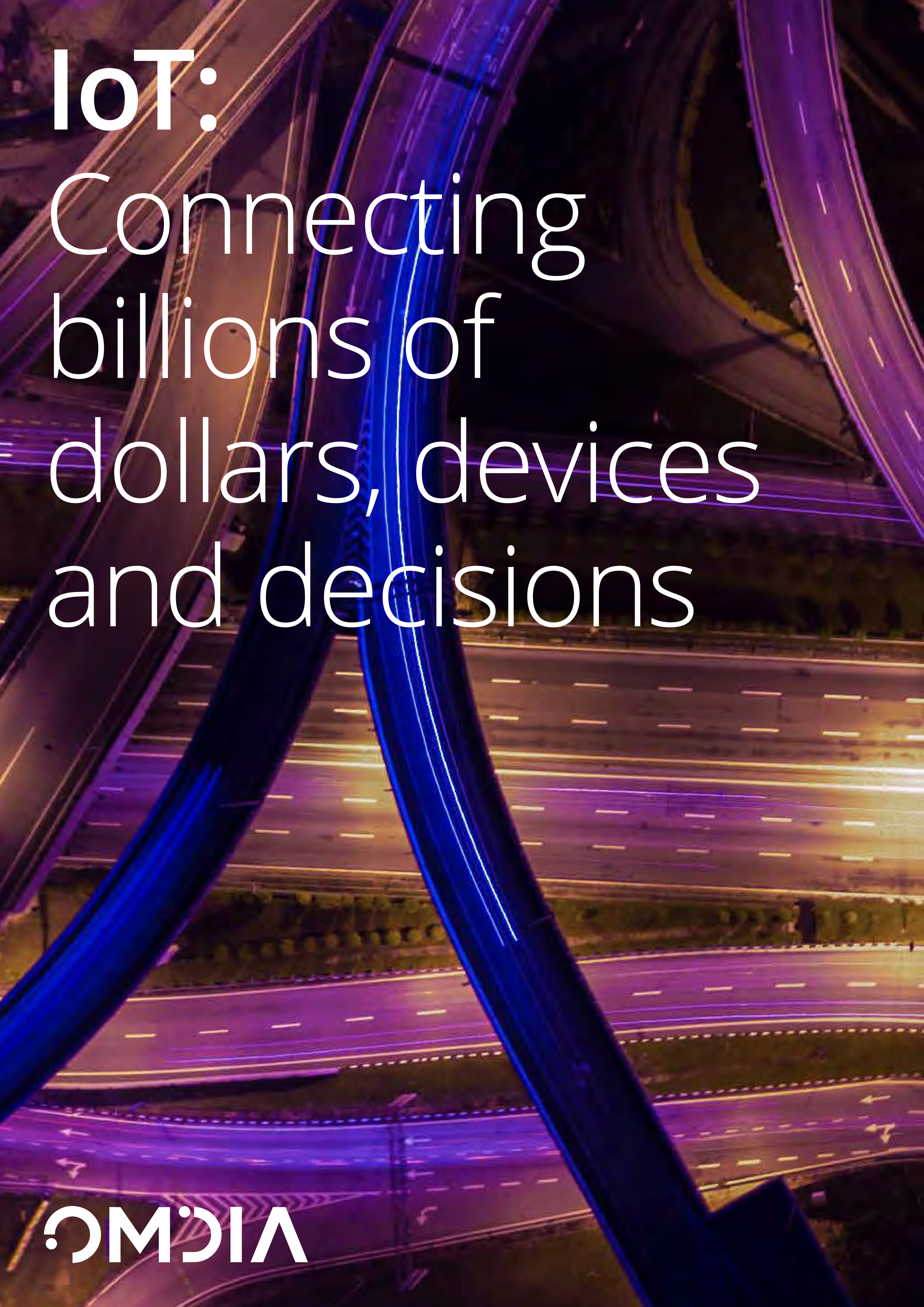


IoT: Connecting billions of dollars, devices and decisions

OMDIA

Table of Contents

IoT: Connecting billions of dollars, devices and decisions

Measured in billions of dollars, devices and even decisions, IoT is moving beyond the hype and much more importantly, is playing a growing role to counter the COVID-19 threat. IoT represents a broad technology shift for all participants in the technology, media and telecommunications (TMT) value chain. This shift is and will have even broader implications, affecting seemingly unconnected markets ranging from industrial manufacturing to integrated circuits, from connected cities to consumer electronics and beyond.

Covering diverse areas extending from modules and chipsets, to 5G, to AI and cybersecurity, and from automotive to industrial and consumer markets, this indispensable IoT analysis, now in its fourth annual edition, is produced by Omdia—the new technology, media, and telecommunications research brand that is connecting the dots, revealing risk, identifying business opportunities, rethinking business practices and delivering the diligence that is essential to make decisions of any scale.

IoT—Moving beyond the hype to realistic, profitable adoption

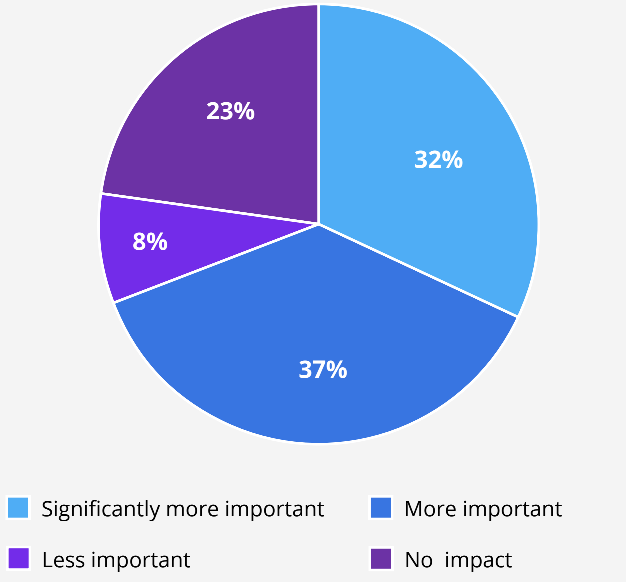
Joshua Builta
Research Director, AI & IoT Pillar

In 2020 the COVID-19 pandemic has brought about unexpected and unprecedented change for businesses and societies throughout the world. One thing that was apparent even in the early days of the pandemic was IoT could be part of the global fight against the virus. A range of IoT applications have been employed to prevent the further spread of COVID-19, while also treating those unfortunately infected. In the early days of the pandemic, 5G connected robots delivered medicine and monitored the condition of patients in field hospitals in China, while drones delivered essential medical supplies and helped enforce stay at home measures. More recently thermal cameras have become commonplace in public places ranging from gyms, schools to retail stores. Going forward, IoT is expected to play a big role in vaccine cold chain monitoring assuring the supply is safe and reliably transported to communities throughout the world.

Of course, these IoT use cases, which have the potential to impact the health and wellbeing of society, outweigh the influence of technology in areas of business. That said, it is also clear there has been a tremendous impact from the pandemic in how businesses will use technologies such as IoT, as they respond to the new unanticipated challenges. IoT has already played a significant role in helping to ensure business continuity through applications such as remote asset monitoring. Further as companies look to re-enter somewhat normal working conditions, IoT is set play an imperative role in creating a smart and safe workplace. This could include biometric screening linked to access control, monitoring employee movement to avoid overcrowding and enable contact tracing, and sensors to ensure air quality.

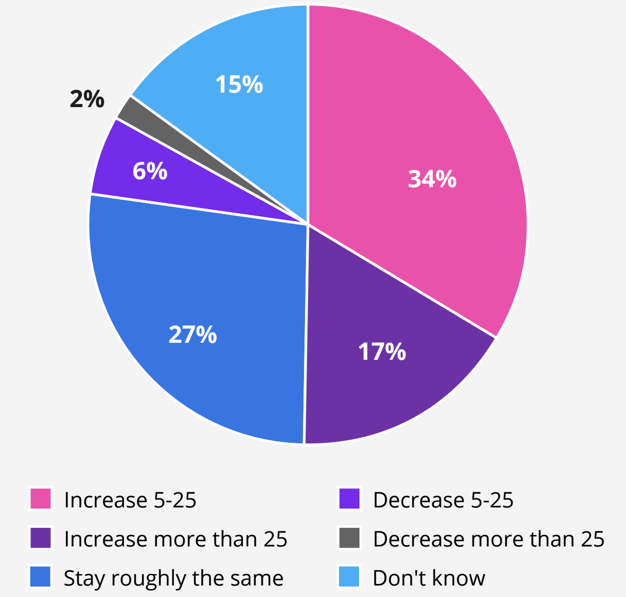
The full impact of the virus on business and technology is still being determined. However, Omdia does believe that many of these changes will ultimately be transformative. They will not be unlearned. Instead they will become the new way of doing things. This suggests that the importance of IoT in our home, in our workplace, and in our entire society is set to grow in the years to come.

What has been the impact of COVID-19 on the relative importance of IoT over the next 18 months?



Source: Omdia 2021.

How do you expect your IoT budget to change by 1Q21?



Source: IoT World Today IoT Adoption Survey.

Strong indications of increased enterprise spending in wake of COVID

For years, IoT solutions have delivered clear value to enterprises through improving efficiency and productivity, enabling cost savings, and enhancing customer experience. Omdia believes there are strong indications that demand for such benefits has been accelerated by COVID-19. According to the results from the most recent Omdia ICT survey, nearly 70% of respondents noted that IoT would be more important to their business in the next 18 months.

Importantly, it appears that prioritization of IoT by enterprises will be supported by investment. A separate survey conducted by Informa's IoT World Today indicates that enterprise investment in IoT is set to grow in the first half of 2021 with over 51% of enterprises surveyed indicating they believed their IoT budgets would increase. In fact, nearly 17% of those respondents stated they expected this increase to be a significance, meaning 25% more than what they spent in 2020.

Framing these developments is the fact that the IoT market still has plenty of room to grow. According to the most recent Omdia's IoT Enterprise Survey, only 29 percent of organizations with more than 50 employees have deployed any IoT solutions. The IoT market must now progress to the next phase: scaling up through the wider commercialization of simple IoT propositions such as asset tracking, alongside development of more complex IoT solutions that will entail the use of complementary technologies, including 5G, AI, IoT, and cloud and edge computing. The confluence of these technologies will continue and provide enterprises with ways to better manage and gain value from their IoT solutions.

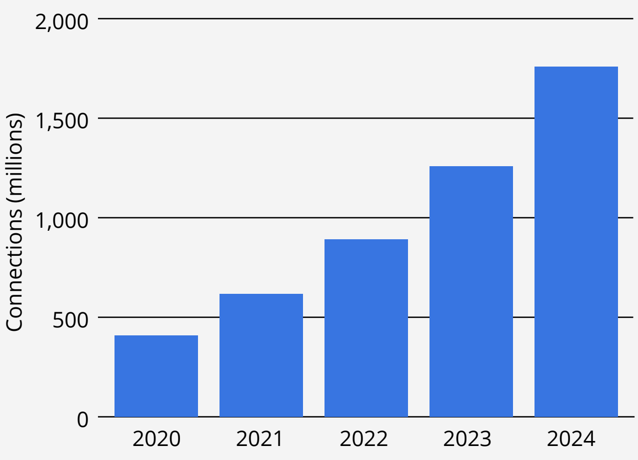
IoT evolution will be reinforced by 5G, LPWAN, AI, and DEPs

It is critical to understand that the readiness and impact of IoT will rapidly change as it converges and become more interconnected.

5G is an example of a technology that will eventually augment IoT and fuel greater innovation and industry disruption. However, Omdia does not believe this transformation will occur in 2021. Ubiquitous 5G network coverage, finalization of some of the most relevant IoT aspects of the technology and maturation of its component ecosystem still need to occur. However, 2021 will see increased enterprise investment, planning, and trials of the IoT applications powered by 5G. This marks a critical and necessary step that must be taken before wider use of technology occurs, especially in segments—such as manufacturing—where use of cellular IoT has previously been largely non-existent. Omdia expects these steps will help drive tremendous growth in 5G in IoT starting in 2023.

Serving a bridge to 5G will be licensed and unlicensed LPWAN (low-power wide area networks). These technologies offer a relatively simple, cost-effective option to connect IoT devices while drawing on minimal power consumption. While adoption of LPWAN have been slower than expected, these technologies will clearly be a growing market in the years to come. In fact, Omdia expects LPWAN connections to increase from 409 million in 2020 to nearly 1.8 billion by 2024.

LPWAN Connections - Global



Source: Omdia 2021.

Of course, connectivity is just one aspect on an IoT solution. A connected device generating a massive amount of IoT data does not create by itself create value. Appropriate tools are needed to manage, securely store, and process data, for its value to be realized. This is where edge cloud architectures and AI solutions will come into play, as more sophisticated IoT use cases require lower latency and more complex processing.

Access to data is another critical aspect of the evolution of IoT. In this regard, Omdia expects IoT Data Exchange Platforms (DEP) to play a critical role. These platforms, which essentially allow for the sharing and reuse of IoT data between organiza-tions, will let various data consumers to combine (or “mash up”) data from many different data sources in innovative ways to provide unforeseen value. A useful analogy is the smart-phone app market—in which the reuse of the smartphone data (“platform”) by third-party app developers have greatly increased innovation and customer options. Omdia predicts that data exchanges have the potential to unleash similar innovation in the IoT market.

Cybersecurity concern remain paramount

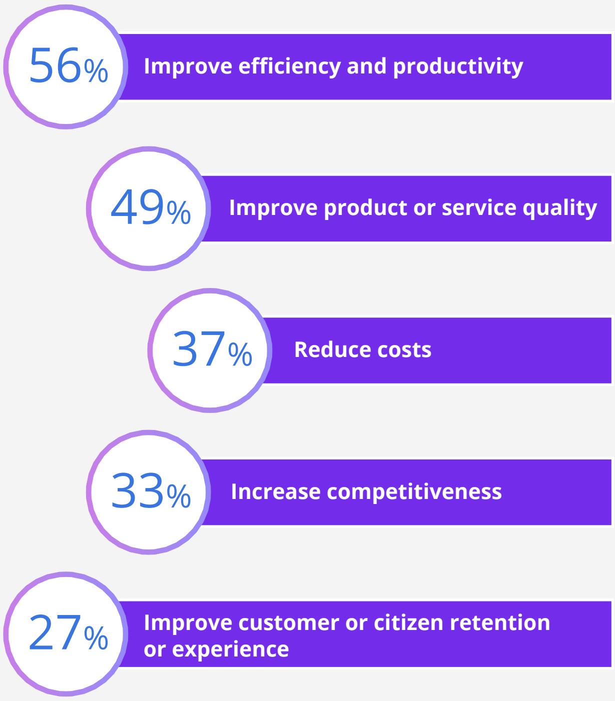
Whether it is a municipality adopting a smart city initiative, a manufacturer trying to connect their factory floor, or a healthcare provider looking to offer remote patient, security concerns are a common thread throughout IoT adopters. In fact, it is the diversity of IoT itself that represents its greatest security handicap. As the variety of devices continues to propagate, while also growing exponentially in volume and scale, the challenge of effectively and securely managing them (and their respective data) becomes a far more complex endeavor. It is therefore no surprise that in the most recent Omdia IoT Enterprise survey, enterprises deploying IoT identified IoT security as their primary challenge.

There are promising signs in the area. Security safeguards are now more commonly “baked into” IoT solutions rather than being treated as an afterthought as they were often in the past when there was more of a “connect first, security later” attitude in industry. The results of this are demonstrated by the revenues generated from IoT cybersecurity solutions which spans disciplines such as device management, data management and identity access management. Altogether these revenues are expected to grow to about $180m in 2024, up from just $68m in 2020.

The threat and resulting concern from enterprises on IoT cybersecurity is not going to away anytime soon. In fact, cyber criminals have attempted to capitalize on the chaos introduced by COVID-19, for instance by developing targeted phishing campaigns. Increased use of IoT in healthcare too will undoubtedly put that sector in the crosshairs of malicious actors and will represent one of the greatest drivers for IoT cybersecurity developments in the near future.

Solving real-world problems and effective partnering will drive IoT success in 2021

What is your organization's main goal in deploying IoT?

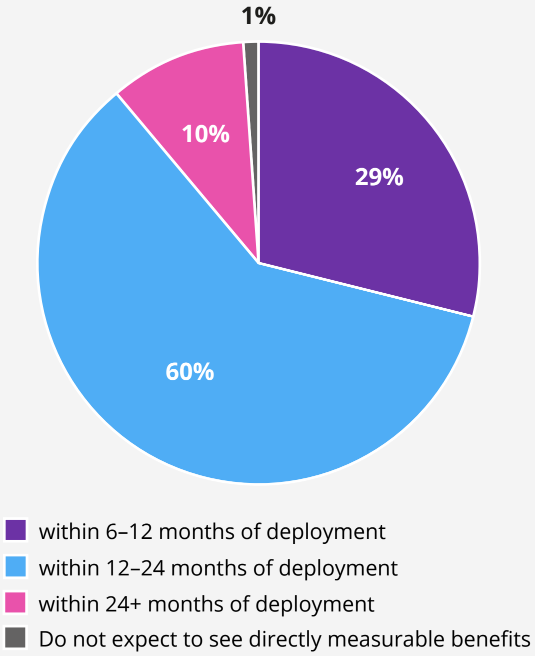


Source: Omdia 2021.

At the end of 2020, Omdia projects the worldwide installed base of IoT devices stands at nearly 28 billion. As strange as it may seem, even at this immense size the market is still maturing. The ecosystem is still a highly fragmented and complex, and while IoT relies on horizontal technologies and capabilities, it's also still the case that vertical propositions are key for connecting with end users. Effective partnering and collaboration can support the development of compelling end-to-end vertical solutions.

Providers must not focus on selling technology but instead offer clear answers and solutions that solve the most glaring pain points for enterprises. Omdia's IoT enterprise study indicates the goal of most IoT deployments is to improve efficiency and productivity, not open new revenue streams. Moreover, four of five enterprises expect measurable benefits directly from their IoT deployment within 24 months. These goals and timeframes must be kept in mind when building IoT solutions; focus on solving the manageable, well-defined to begin with and use that to get buy-in from the wider organization.

What timeframe do you expect for your organization to realize measurable IoT benefits?



Source: Omdia 2021.

While the circumstances are unfortunate, the wide and significant role IoT has played in the response to the COVID-19 underscores its clear ability to quickly such solve immediate real-world problems. This lesson should be carried forward by all in the ecosystem and give confidence to all that IoT can drive innovation, disrupt industries, and fundamentally improve society and businesses in the future.

> “In many cases the changes brought about COVID will become the new way of doing things. This suggests the importance of IoT in our home, in our workplace and throughout society is set to grow in the years to come.”

5G to generate nearly $9tn worth of economic output sales enablement in massive IoT and mission-critical services by 2035

Joshua Builta
Research Director,
AI & IoT Pillar

Julian Watson
Principal Analyst, IoT

The proliferation of 5G technology represents one of the biggest economic opportunities of the 21st century, with the wireless standard set to unleash $13.1tn of global economic output by 2035. Two-thirds of this opportunity lies in mission-critical services and massive Internet of Things (IoT) deployments, with the two sectors collectively accounting for $8.98tn worth of 5G sales enablement by 2035, according to IHS Markit and Omdia in a report published in November 2020. For companies aiming to capitalize on this growth, it will be critical to understand how 5G's evolving IoT technology can address their operational challenges and help them attain their strategic objectives.

The massive opportunity in massive IoT

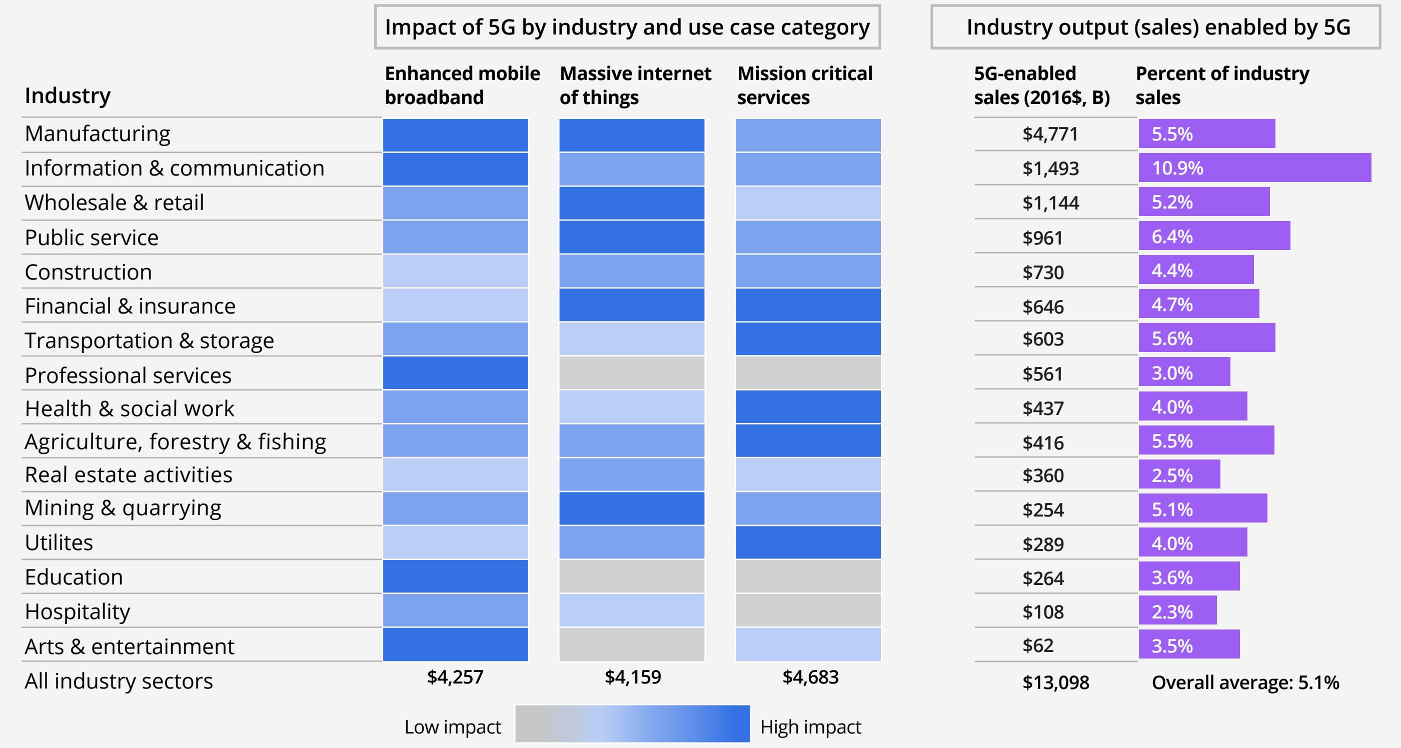
In the near term, the impact of massive IoT will be seen in existing IoT use cases, such as asset tracking, which has widespread relevance across many industries, including manufacturing, transportation and storage, and mining and quarrying. In the longer term, 5G's enhancements related to massive IoT, including power savings and a greater connection density, will open opportunities in other areas, such as smart cities, smart agriculture, and remote monitoring.

Mission-critical services set for 2021 debut

Release 16 and 17 from the 3GPP standards organization on 5G features standardization efforts concerning ultra-reliable low-latency communications (URLLC). These efforts will allow the initial proof-of-concept and small-scale deployments of 5G mission-critical services starting in 2021.

The organization's demanding technical requirements on 5G availability and latency mean that many industries will initially take a cautious approach to deployment of the next-generation mobile standard. However, the widespread usage of devices like drones and autonomous vehicles across many industries, such as agriculture, forestry, and fishing, construction, and transportation and storage, will drive adoption in the longer term.

5G will enable $13.1tn in global sales activity in 2035



Industry	5G-enabled sales (2016$, B)	Percent of industry sales
Manufacturing	$4,771	5.5%
Information & communication	$1,493	10.9%
Wholesale & retail	$1,144	5.2%
Public service	$961	6.4%
Construction	$730	4.4%
Financial & insurance	$646	4.7%
Transportation & storage	$603	5.6%
Professional services	$561	3.0%
Health & social work	$437	4.0%
Agriculture, forestry & fishing	$416	5.5%
Real estate activities	$360	2.5%
Mining & quarrying	$254	5.1%
Utilites	$289	4.0%
Education	$264	3.6%
Hospitality	$108	2.3%
Arts & entertainment	$62	3.5%
All industry sectors	$13,098	Overall average: 5.1%

	Enhanced mobile broadband	Massive internet of things	Mission critical services
All industry sectors	$4,257	$4,159	$4,683

Source: IHS Markit.

The big picture for 5G

5G's impact on the IoT and on mission-critical services reflects the transformational nature of the technology. Far more than providing just an improved mobile experience, 5G will transcend the communications field and fundamentally alter how a vast and diverse group of industries operate. This phenomenon will generate massive and sustainable economic benefits across all sectors of the global economy, generating the aforementioned $13.1tn worth of global economic output, according to a study conducted by Omdia and the IHS Markit Economics & Country Risk service.

The goal of the study was to understand what 5G enables industries to do or sell, above and beyond what 4G can support. Furthermore, the study sought to quantify the revenues generated from those targeted 5G use cases throughout the value chain. For example, autonomous driving will generate new sales transactions for various entities across the supply chain, including semiconductor suppliers manufacturing 5G chipsets, suppliers of telematic control units (TCUs), the automobile manufacturers, and—potentially— ridesharing companies such as Uber and Lyft.

Quantifying the "5G Economy"

To quantify the "5G Economy," the Omdia team, in partnership with Qualcomm, assessed 21 different use cases for 5G technology across enhanced mobile broadband (e.g., indoor and outdoor wireless broadband, fixed wireless broadband, augmented reality, and extended mobile computing); massive IoT (e.g., asset tracking, smart agriculture, smart cities, energy/ utility monitoring, and remote monitoring); and mission- critical services (e.g., autonomous vehicles, drones, industrial automation and medical). The impact of each use case was then modeled on 16 major industry sectors.

The findings from the study were significant. The $13.1 trillion in sales enablement is nearly equivalent in current levels in US consumer spending of $13.9 trillion, and comparable as well to the combined spending in 2018 of $13.4 trillion by consumers in China, Japan, Germany, the UK, and France.

The $13.1tn in sales enablement in 2035 is only slightly lower than the $13.2tn forecasted in a previous report from November 2019, before the COVID-19 pandemic struck. Although the 5G standardization process was slowed by the spread of COVID-19, continued 5G deployment, driven by China and the release of new devices mean that the 5G ecosystem has continued to innovate and commercialize despite the challenges of supply chain disruption and restrictions on people movement imposed in many countries. The requirement to be nimble has accelerated enterprise digital transformation efforts during the pandemic and emphasized the vital importance of robust connectivity and the transition to new, flexible ways of working and delivering services, enabled by technology.

Other key findings from the study include:

By 2035, the 5G value chain alone will drive $3.8tn of economic output and support 22.8 million jobs. This is approximately the combined revenue of the top 10 companies on the 2019 Fortune Global 1000—a list that includes Walmart, Sinopec Group, Royal Dutch Shell, China National Petroleum, State Grid, Saudi Aramco, BP, ExxonMobil, Volkswagen, and Toyota. Fortune estimates these companies employ almost 6.5 million workers. Thus, for the same level of output, the 5G value chain will support 3.4 times as many jobs.

From 2020 to 2035, it is anticipated that the collective investment in R&D and CAPEX by firms that are part of the 5G value chain within just seven countries (China, United States, Japan, Germany, South Korea, France, and United Kingdom) will average over $260bn annually. For the 2020–2035 period, it is forecast the global real GDP will grow at an average annual rate of 2.7%, of which 5G will contribute almost 0.2%. From 2020 to 2035, the annual GDP contributions of 5G, as shown in the following graph, will total almost $2.9tn. Keys to success in the 5G era.

Across every industry vertical and geography, enterprises of all types are seeking to remain relevant and profitable in highly competitive markets, while facing constant disruption from challenges including digital-first entrants, changing customer behavior, and new regulatory and environmental requirements. Companies are becoming aware that the first iterations of 5G will deliver greater bandwidth and lower latency than previous iterations of cellular technology. They need access to more information and more proof points as to how 5G will evolve; what type of performance levels it will support compared to other wireless and wired technologies; and most importantly, how 5G's capabilities may help address their operational challenges and strategic objectives.

Enterprises should engage with 5G vendors to understand the benefits the technology could deliver to their businesses. Internal discussions on what 5G can bring to the table will also be key, and these must involve not only IT and operational technology (OT) teams, but also strategic and client-facing functions.

> “5G’s impact on the IoT and on mission-critical services reflects the transformational nature of the technology. Far more than just providing an improved mobile experience, 5G will transcend the communications field and fundamentally alter how a vast and diverse group of industries operate.”

Device vendors focus on total cost of ownership and edge capabilities as IoT installed base swells to 28 billion

Julian Watson
Principal Analyst, IoT

With the global installed base of Internet of Things (IoT) devices expected to approach 28 billion in 2021, the IoT market's focus increasingly is shifting away from upfront hardware expenses toward the total cost of ownership (TCO) of these systems.

Over a five-year period, the operating expense (OPEX) for a common type of IoT device can account for nearly half the product's TCO, according to an estimate from Omdia. With device life spans extending well beyond that time frame, the balance of TCO will shift toward OPEX and away from the upfront device cost.

As a result, device vendors this year are expected to provide customers with more transparent TCO data, offering comprehensive OPEX and capital expenditure (CAPEX) information to help customers understand, predict, and manage TCO during the entire lifetime of their IoT devices.

TCO promotes IoT simplification

The embrace of TCO conforms with major trends in the IoT market. Over the past two years, "simplifying the IoT" and "edge in IoT" have become familiar themes at IoT events. For some vendors, simplification has meant reducing or eliminating the need for programming skills among enterprise users of their solutions. For others, simplification has involved working with partners to develop IoT solutions that pre- integrate several components of a solution in a single package.

On the edge, applications players are focusing on the capability of edge compute to enable low-latency IoT applications. From an analytics perspective, edge in IoT is all about performing on-device artificial intelligence (AI), or extracting data from constrained edge devices and ingesting it into the cloud and into core enterprise systems.

These two trends will come together in 2020, opening new opportunities for providers.

In Omdia's view, one of the most important elements of IoT simplification—clear IoT pricing models—still has not been fully addressed by vendors. With edge for IoT now in the mix, pricing models will need to incorporate these new capabilities a way that can be easily understood and digested by customers.

Understanding, predicting, and managing TCO can be notoriously difficult with IoT projects, and is a reason why many do not go beyond the proof-of-concept stage. By providing key TCO data, vendors can aid these processes, promoting IoT deployment.

Examining IoT device TCO

The chart below shows the TCO over five years for one of the most common types of IoT solutions: a cellular-enabled asset tracker.

The chart picks four core sources of TCO: the upfront (CAPEX) cost of the device; the recurring OPEX costs related to device and data management; connectivity management; and connectivity service fees.

Omdia assumes a representative device cost of $100. This reflects the typical need for ruggedization, an industrial-grade battery, support for several cellular bands, and GPS for location services.

Over the five-year life span of the device, the device on its own accounts for 53% of the TCO. In comparison, the OPEX costs distributed across device and data management, connectivity management, and connectivity service fees account for 47% of the total cost. Based upon ongoing development work by standards bodies, semiconductor vendors, and battery vendors, battery and device life span extend well beyond five years.

Over time, therefore, Omdia believes the balance of TCO will shift toward OPEX. This trend increases the need for vendors to provide more transparent, and ideally flexible, OPEX pricing.

In summary, Omdia estimates that the OPEX costs—including device and data management, cellular connectivity service, and connectivity management—account for nearly half of the TCO.

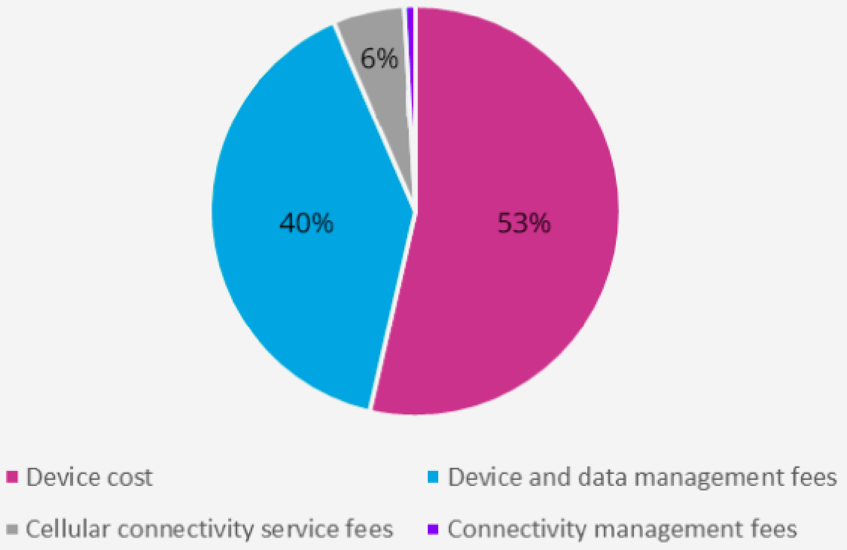
Vendors take on IoT TCO

Sierra Wireless and Amazon Web Services (AWS) are two good examples of IoT technology vendors that have sought to improve the transparency of ongoing costs while leveraging edge capabilities. For Sierra Wireless, its old strategy has been to develop integrated solutions that brought together hardware, connectivity, and platform capabilities.

In October 2019, the company launched Octave, a solution particularly targeted at cellular low-power use cases, allowing users to "securely extract, orchestrate, and act on data from your equipment to your cloud." One element of Octave consists of IoT infrastructure, such as edge devices like gateways, modules, or an open-source hardware platform; connectivity services; and connectivity and device management via the Sierra Wireless AirVantage IoT platform. The other element is data orchestration, or extracting data from edge devices, processing events, and filtering data.

To simplify pricing, several sources of OPEX costs within Octave are bundled into two monthly fees: a platform fee of $1 per device per month that includes low-power wide-area network

IoT connected devices 5-year total cost of ownership



Source: Omdia 2020.

(LPWAN) access, network and device management, heartbeat, and up to 4 over-the-air (OTA) updates per year; and a messaging fee of $1 per 1,000 messages. These messages can be pooled across all devices, a concept relatively new to cellular IoT, and one that mimics consumer-shared data plans.

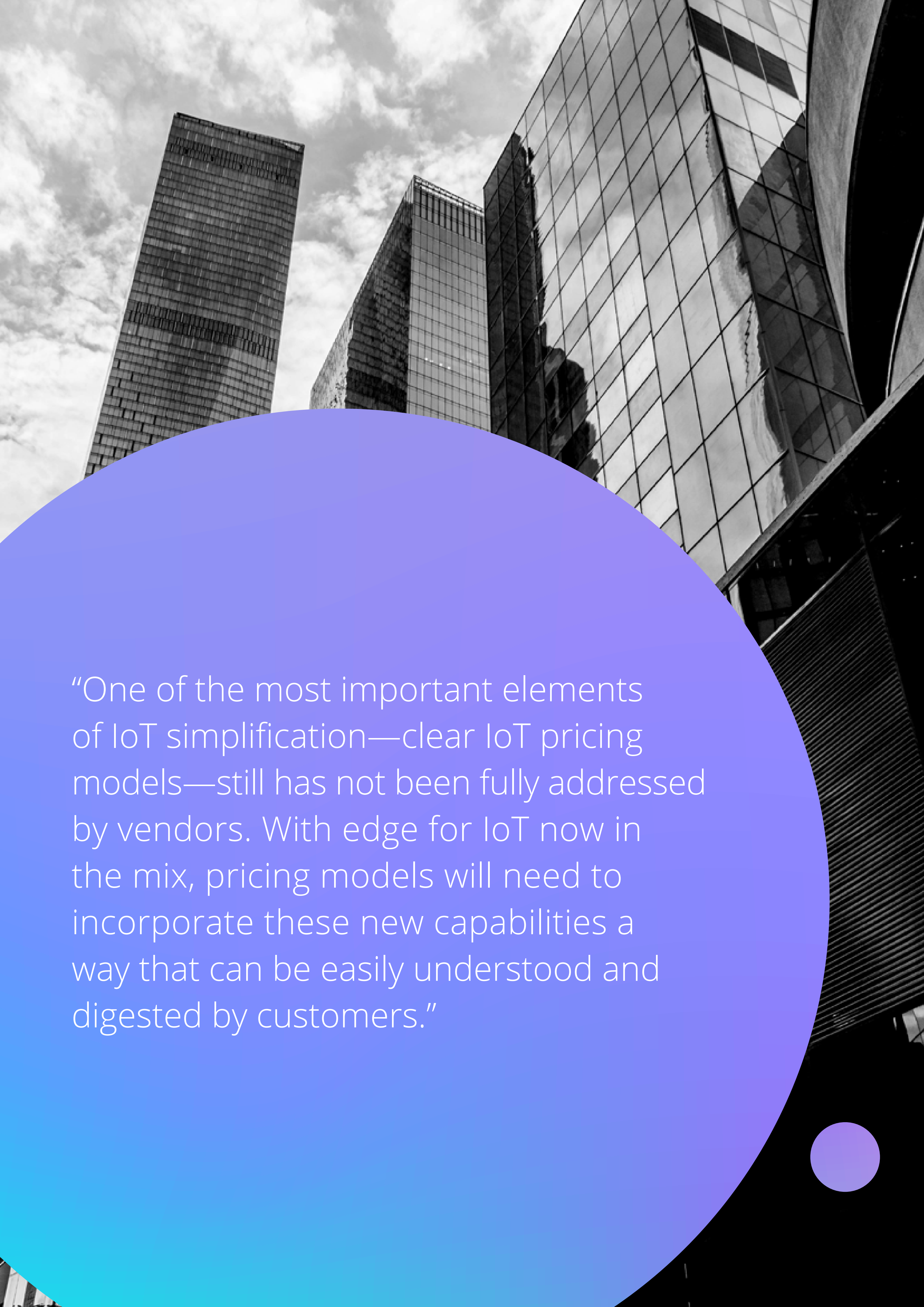
Meanwhile, cloud leader AWS is also introducing simplified pricing for IoT customers. In late 2019, AWS announced a new pricing model for its IoT SiteWise offering, a managed service designed to collect, store, organize, and monitor data from edge industrial equipment, such as robotic arms. Previous AWS pricing for data ingress and egress had been based on the amount of data ingested or scanned, while pricing for data processing was based on the amount of data used within computations. For the new model, pricing is no longer based on data volumes but instead is calculated on the number of both data ingress and data egress messages, as well as on the number of data-processing computations.

Recommendations

Oftentimes, supply-side vendors and industrial enterprise customers apprehend IoT data differently. On the one hand, telecoms operators and module vendors are primarily concerned with providing a resilient, secure communications path for IoT data from the device and over the network. Cloud companies, for their part, are most concerned with planning for enough storage and processing power to handle large volumes of IoT data.

On the other hand, industrial companies are more concerned with the frequency, type (i.e., content), and reliability of alerts transmitted from their edge assets. Transparency around the costs related to these functions can help them assess the financial implications of shifting from manual, regular inspections of equipment to interventions or predictive maintenance, based on the remote monitoring of equipment. As a result, pricing based on volumes—whether for data traffic traveling over an operator network, or the amount of data that is either processed or computed—is not an optimal way for industrial companies to assess TCO.

“Speaking the language of customers” is a well-known mantra, but vendors need to go beyond this approach to align their IoT pricing models with the processes and pain points of their customers. The moves by Sierra Wireless and AWS are good examples demonstrating this point. For 2020 and beyond, aligning pricing models and TCO to the enterprise and budgeting processes of different verticals will be a key driver in making IoT adoption profitable for business and industry.



“One of the most important elements of IoT simplification—clear IoT pricing models—still has not been fully addressed by vendors. With edge for IoT now in the mix, pricing models will need to incorporate these new capabilities a way that can be easily understood and digested by customers.”

LPWAN demand set to quadruple by 2024 as costs decline and use cases materialize

Christian Kim
Senior Analyst,
IoT & Connectivity

Pablo Tomasi
Senior Analyst, IoT

Despite the IoT market's slower-than-expected uptake in 2020 of low-power wide-area networks (LPWANs), the networking technology is positioned for strong growth in the coming years, with global connections rising by a factor of four between 2020 and 2034.

The number of LPWAN connections worldwide is set to increase to 1.17 billion in 2034, up from 228 million in 2020, according to Omdia's latest forecasts. Uptake will accelerate as communications service providers (CSPs) and LPWAN vendors demonstrate compelling use cases and clear cost advantages for the technology.

The characteristics of LPWAN—including low cost, long battery life, extended coverage, and low-bandwidth—appear to be a perfect match for many IoT use cases. However, LPWAN's slow uptake in markets outside of China comes as a reminder that a successful IoT strategy cannot rely on a single technology, and that enterprises do not adopt or adapt to new technologies as quickly as consumers.

LPWAN's challenges also highlight the fact that linking new IoT technologies to IoT use cases is a critical element in driving enterprise demand.

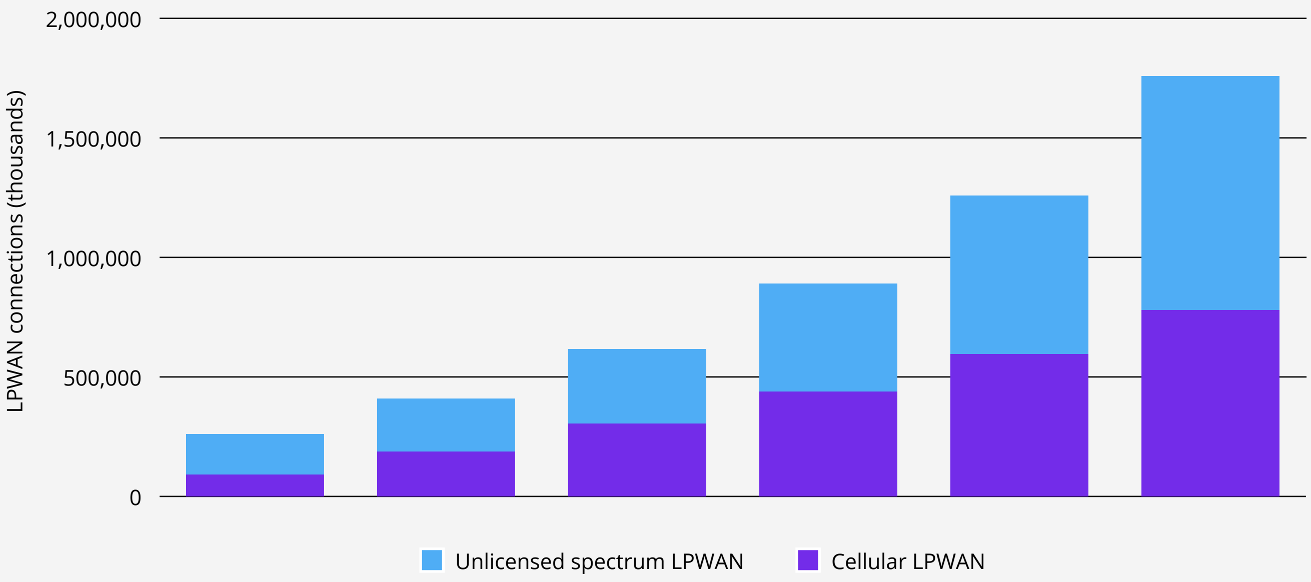
Slow growth of licensed spectrum LPWAN shows IoT success is not assured

Mobile operators have been pushing Narrowband IoT (NB-IoT) and LTE-M as core LPWAN technologies using licensed cellular spectrum, to address the massive IoT market and drive revenue growth. However, the rollouts in many cases have been slow and have only covered limited geographic areas, even though national coverage is now available in many nations, including the US, China, South Korea, South Africa, Brazil, and much of Europe.

Development of the cellular LPWAN device and module ecosystem has also been slower than expected. Prices remain relatively high, in effect eliminating a key selling point for the technologies. However, module prices are declining as more players enter the market, which should help generate sales momentum this year.

aThese factors are further exacerbated by the inability of operators to provide clear and unique use cases for both LTE-M and NB-IoT, as well as for their eventual 5G versions using "massive MTC," or machine-type communication.
To be sure, suitable use cases have been found, including smart metering—in particular, water and gas metering, asset monitoring, smart urban transport such as connected bikes

LPWAN connections growth forecast (thousands)



Source: Omdia 2021.

and scooters, and smart home/smart building devices. In China, for instance, smart metering deployments using NB-IoT have exceeded 10 million units.

For now, however, most low-bandwidth requirements can still be adequately met by 2G or 3G cellular, which possess better device and module availability while also bearing similar costs; or by unlicensed spectrum LPWAN alternatives.

China serves as NB-IoT showcase

For NB-IoT, the Chinese market remains an exception, providing the only significant success story so far. Omdia of 2019, China accounted for more than 72% of total licensed spectrum LPWAN connections worldwide, with most of those connections—just under 90 million—utilizing NB-IoT.

The success of NB-IoT in China can be attributed to various factors, including Beijing's support of the technology; the commitment to NB-IoT investment and rollout from China Mobile, China Telecom, and China Unicom—China's three state-run telecom providers; and the rapid development of a large ecosystem. In turn, the NB-IoT ecosystem in China is supported not only by major tech vendors such as Huawei, but also by a large constellation of Chinese device and chipset manufacturers.

> "LPWAN's challenges highlight the fact that linking new IoT technologies to IoT use cases is a critical element of driving enterprise demand."

Developments and adoption trends in cellular LPWAN in China are likely to be well ahead of those in the broader global market for the next several years.

Improved LPWAN ecosystem to drive growth this year

The LPWAN ecosystem will slowly improve in 2020, and device and module costs will continue to decline, which will help propel sales. CSPs and their vendor partners must continue educating the market on why and when LTE-M and NB-IoT are most suitable, while ensuring that their LPWAN-based offerings are linked to use-case-based solutions, rather than simply being offered as connectivity technologies.

The 2G and 3G switch-off in some markets will provide a further boost to NB-IoT and LTE-M, as CSPs look to migrate IoT customers using 2G and 3G onto new, low-cost alternatives. Players should also consider driving market interest through new pricing models, such as the flat all-inclusive IoT rate offering provided by mobile virtual network operator (MVNO) and platform provider 1NCE in Europe for its low-bandwidth IoT services.

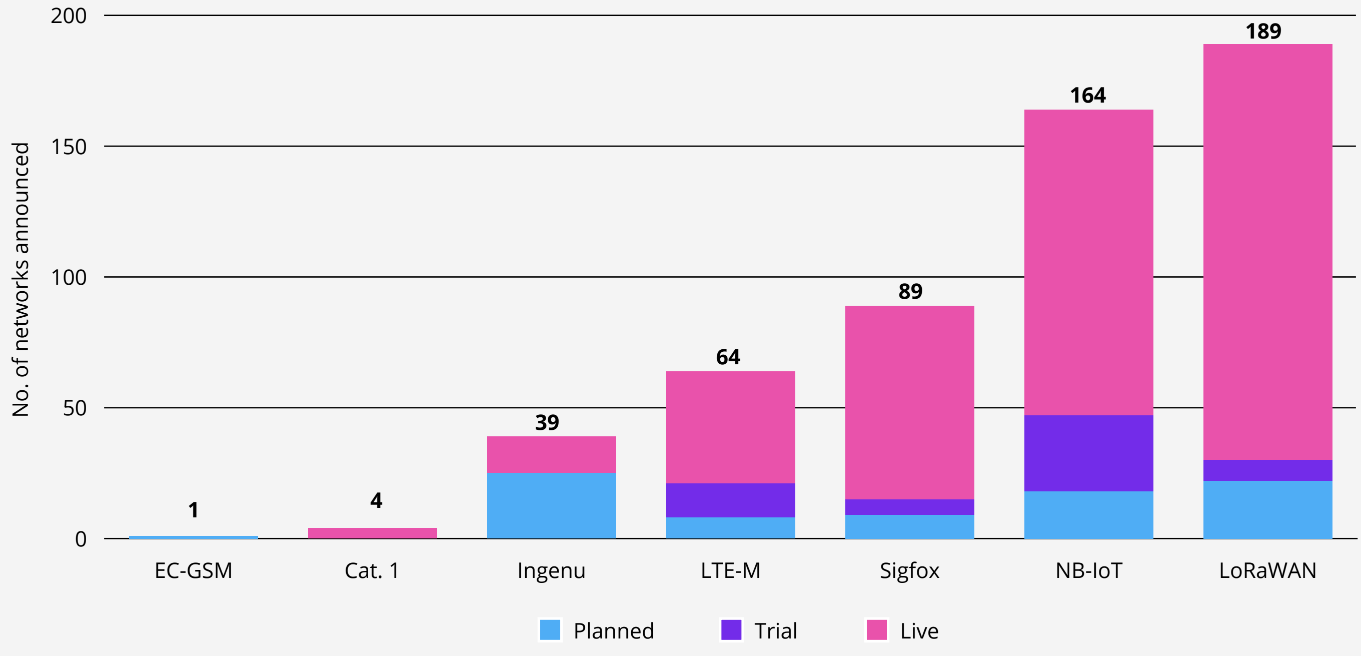
Challenges also remain in coverage and roaming, even though CSPs have been acting on both issues. In June 2019, Orange, AT&T, Swisscom, and KPN announced the implementation of LTE-M roaming on their networks across several European countries and North America. In October of the same year, Vodafone and AT&T announced they signed an NB-IoT roaming agreement that also included the two operators agreeing to LTE-M network roaming in the US and the Netherlands. In April 2020, Deutsche Telekom, Swisscom, Telia, and Vodafone signed NB-IoT roaming agreements. Through signing the NB-IoT roaming agreement, Deutsche Telekom expanded its NB-IoT availability to 18 countries in Europe. Overall, IoT roaming for NB-IoT or LTE-M has important advantages for applications like asset tracking, which may need connectivity across multiple countries. Yet more needs to be done, and more announcements are expected this year on NB- IoT and LTE-M roaming agreements.

Unlicensed spectrum LPWAN drives ahead

Unlicensed spectrum LPWAN options—especially LoRaWAN, and to a much lesser degree, Sigfox—have also been eating up some of the market opportunity for LPWAN because the technologies are cheaper at present. Moreover, because the technologies use unlicensed spectrum, companies can deploy them more quickly and easily, even though they are not interoperable with cellular.

Among unlicensed LPWAN technologies, LoRaWAN is the frontrunner. While many LoRa networks are private, public LoRa networks can now be found in 162 countries, with the

Number of LPWA deployment announcements by technology through Q4 2019



Source: Omdia 2021.

technology currently supported by 148 service providers globally, according to the LoRa Alliance.

For its part, Omdia expects LoRa to continue expanding its reach in 2020, supported by the LoRa Alliance, which currently counts more than 500 member companies; and by an ecosystem of more than 50,000 developers. In a recent briefing with Omdia, LoRaWAN technology provider Semtech reported it estimates more than 150 million LoRaWAN nodes are live, including those in private networks.

Recommendations

CSPs and vendors can drive the uptake of LPWAN technologies by demonstrating unique use cases and clear cost advantages, as well as by continuing to build out coverage and roaming agreements.

All told, availability of the technology is not enough on its own to drive growth of the LPWAN market, but greater scale will help drive down module costs while boosting device availability, resulting in a further push to the market.

Enterprise adopters must also be presented with business cases compelling enough to drive adoption, along with a solid business model that solidifies the case for LPWAN.

IoT platform vendors strike partnerships to capitalize on market's rapid growth

Sam Lucero
Senior Principal Analyst,
IoT Platforms

In a fast-growing and highly fragmented IoT platforms market expected to more than triple in size by 2023, no single player can be all things to all customers. Partnerships are key to success. As a result, the number of announced partnerships between IoT platform providers is on the rise.

The worldwide IoT platform market is set to grow to $70 billion in 2023, up from $20 billion in 2019, according to the Omdia IoT Market Tracker. Growth will be underpinned by partnerships commonly entered into so that complexity in developing and deploying IoT applications can be reduced.

Partnerships take aim at IoT complexity

IoT complexity manifests in several areas, including determining return on investment (ROI); engaging in technology development, such as choosing standards and managing devices over complex networks; and conducting ecosystem development, manifested in the selection of suppliers and distributors.

Complexity increases the risks for IoT application developers and for corporate adopters of IoT technology. The risks include rising costs, unrealized benefits, growing security threats, increased time to market, and failure to achieve a satisfactory ROI.

Such risks have a negative impact on IoT market development. A total of 30% of IoT projects fail in the proof-of-concept phase, according to original survey research conducted by Microsoft. Cisco has published similar research findings.

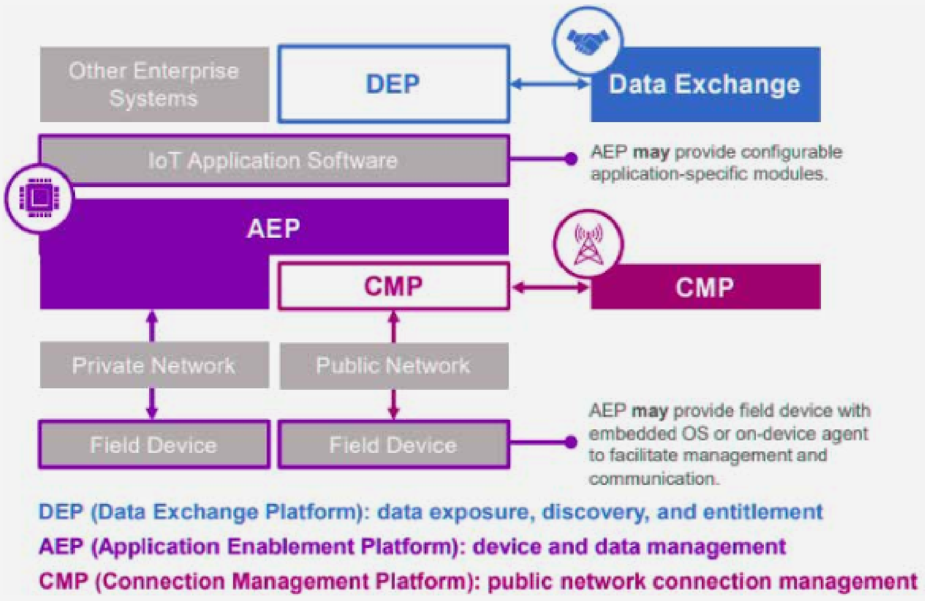
Infrastructure vendors partner up

A common characteristic among IoT platform partnerships is that one of the partners usually is also a cloud infrastructure vendor. This makes sense because in most enterprise IT environments, including the IoT space, cloud infrastructure vendors like Microsoft and Amazon have not only become key suppliers but have also turned into platform providers.

The other partner tends to be one of four types of companies that offer a complementary service to the cloud infrastructure vendor's offering:

- **Vertical specialist**
  A platform vendor that targets a specific vertical or market, such as connected cars, and develops industry-specific expertise in understanding the needs of that vertical or market. For example, in December 2019 Microsoft and Ericsson announced a partnership based on Ericsson's Connected Vehicle Cloud and Microsoft's Connected Vehicle Platform.

Role of IoT Platforms in the application stack


Other Enterprise Systems
DEP
Data Exchange
IoT Application Software
AEP may provide configurable application-specific modules.
AEP
CMP
CMP
Private Network
Public Network
Field Device
Field Device
AEP may provide field device with embedded OS or on-device agent to facilitate management and communication.
DEP (Data Exchange Platform): data exposure, discovery, and entitlement
AEP (Application Enablement Platform): device and data management
CMP (Connection Management Platform): public network connection management

Source: Omdia 2020.

- **Connectivity service provider**
  A platform vendor that provides connectivity-as-a-service over a public network. These vendors include mobile operators and satellite operators. For example, in IoT applications, Microsoft is working with satellite operator Inmarsat; while AWS is working with satellite operator Iridium.

- **Data exchange market maker**
  A platform vendor that focuses on enabling third-party organizations to expose, discover, share, and potentially monetize IoT data. For example, data exchange platform vendor Otonomo has partnered with Microsoft to build services on top of Microsoft Azure and the Microsoft Connected Vehicle Platform.

- **Component vendor**
  A platform vendor that focuses on offering key hardware components, typically connectivity modules and modems, and has developed a strategy of providing a turnkey device-to-cloud capability aimed especially at small- and medium-sized business (SMB) developers and adopters. For example, Sierra Wireless has announced a partnership to connect its Octave platform with Microsoft's Azure IoT Central platform.

Clearly, such partnerships resolve some of the ecosystem development challenges addressed above. Partnerships can also help reduce technology risk through pre-integration and certification of each partner's respective technology with that of the other partner. These partnerships also have the effect of reducing the need and demand for broadly applicable IoT standards.

It is likewise important to note that these partnerships usually are not exclusive. Customers of one partner still could select other, non-partnered suppliers if they so choose.

Ultimately, these types of partnerships will become more common, as platform vendors seek to reduce complexity and the resulting risk for customers.

Recommendations for IoT platform players

IoT application developers and enterprise users evaluating an appropriate IoT platform strategy to adopt should consider the following questions:

- Is technical differentiation achievable by sourcing different platform components individually?
- Should the potential developers and users of the IoT platform rely on pre-integrated, partnered solutions and focus their differentiation strategy on business attributes?

With the IoT platform market continuing to mature as underlying infrastructure for various IoT applications, there will be a decrease in benefit to developers and adopters if they select each supplier individually, rather than by leveraging pre-partnered ecosystems where available. Omdia recommends that most developers and adopters leverage the benefits of these pre-partnered solutions where available, absent a compelling reason to attempt a selection of "best-in-class" suppliers.

“With the IoT platform market continuing to mature as underlying infrastructure for various IoT applications, there will be a decrease in benefit to developers and adopters if they select each supplier individually, rather than by leveraging pre-partnered ecosystems where available.”

IoT moves to the final frontier, with 10 million satellite connections by 2025

Sam Lucero
Senior Principal Analyst,
IoT

The Internet of Things (IoT) has already conquered the earth, with billions of devices everywhere—from cars, to factories, to entire cities. Now the IoT is blasting off into space, with cumulative satellite connections expected to rise to more than 10 million by 2025.

The installed base of satellite IoT connections will increase by nearly a factor of four in the coming years, expanding at a 25% CAGR from 2.7 million units in 2019 to reach 10.3 million units in 2025, according to Omdia.

While satellite IoT will only account for a small proportion of overall IoT connections, it will support critical use cases in industries such as maritime and oil and gas. During the next 10-15 years, standard terrestrial wireless IoT technologies will play a key role in enabling satellite-based IoT connectivity. However, in the near term—or in less than five years—terrestrial wireless technologies will have only minimal impact, accounting for less than 10% of the installed base of satellite-connected IoT devices in 2025, as presented in the chart.

It is important to note that this forecast encompasses directly satellite-connected devices and gateways alone; hundreds or thousands of devices sitting behind the gateway may be potentially excluded.

The new space race

The IoT's conquest of space has gained momentum over the past year, with the launch of several high-profile ventures that comprise the "NewSpace" movement involving the private spaceflight industry. These ventures, including SpaceX's Starlink, Amazon's Project Kuiper, and Softbank-backed OneWeb, are bringing satellite-based broadband Internet access to areas underserved by terrestrial networks.

At the same time, some satellite operators—both established companies and startups—are exploring new opportunities to connect IoT devices. While most rely on proprietary satellite connectivity technologies to support IoT devices, several are starting to leverage terrestrial wireless IoT connectivity technologies in their network strategies.

Terrestrial tech for space connectivity

Terrestrial wireless IoT connectivity technologies—specifically the set of standards comprising LoRaWAN, NB-IoT, LTE-M, and eventually 5G NR Low Power—benefit from scale, compared to proprietary approaches common in the satellite industry. This leads to reduced costs, greater supplier diversity, and easier integration for customers. The benefits have drawn interest from several satellite operators seeking to use terrestrial wireless standards as ground-to-satellite link technology, in place of current proprietary satellite industry connectivity technologies.

While some operators, such as Australia’s Fleet Space Technologies, seek to use terrestrial technologies only for local area networking in conjunction with local gateways containing traditional satellite backhaul links, others intend to replace proprietary satellite connectivity links entirely with terrestrial wireless standards. For example, US-based Ligado Networks has the technical capacity now to support connectivity to an NB-IoT or LTE-M IoT end-device directly from a satellite. No intermediate gateway or proprietary backhaul technology is needed.

Terrestrial IoT faces growth hurdles

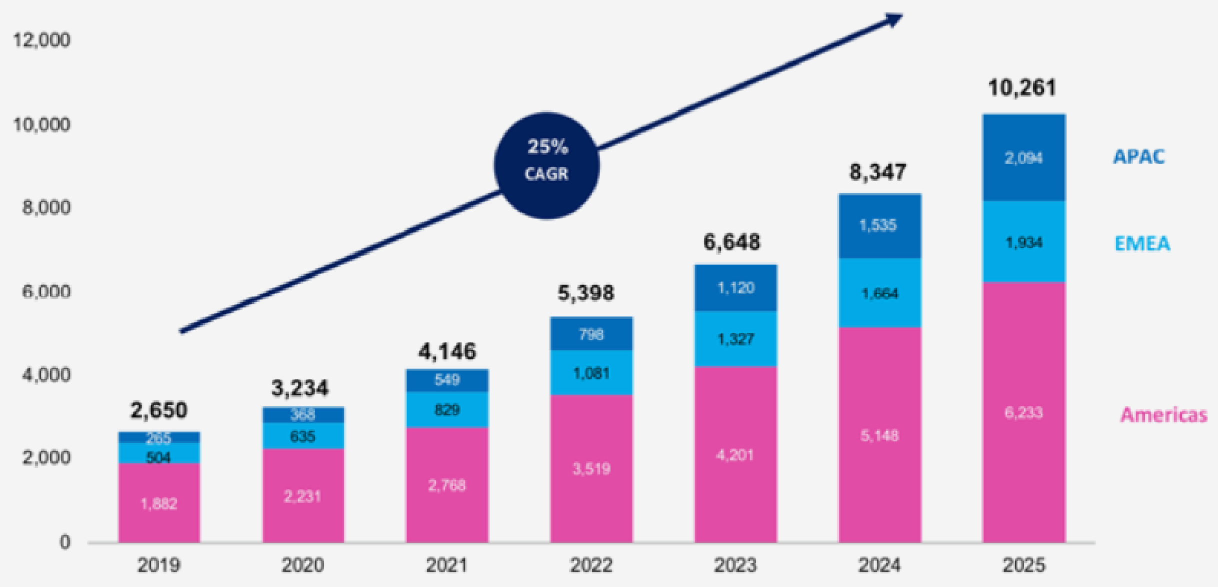
Several constraints stand in the way of short-term growth of satellite connectivity for standard terrestrial IoT technologies.

First, the largest established satellite operators have not jumped on the terrestrial wireless IoT bandwagon. These operators include US satellite companies Globalstar, Iridium, and Orbcomm, as well as French-based Eutelsat and Inmarsat of the UK. Together, the five companies accounted for over 96% of the installed base of satellite IoT connections in 2019, and growing connections at an annual rate of approximately 16%. This implies that new operators using terrestrial wireless technologies would have to grow astronomically to significantly impact the overall mix of IoT connectivity technologies in the short term.

While Globalstar has won approval to use some of its licensed RF spectrum for private terrestrial networks, established satellite operators are sticking with the traditional proprietary technology approach for satellite-to-ground connectivity. These operators have invested significant capital in their existing networks, which already support a rapidly growing base of paying customers. Given their sunk costs—costs that have already been incurred and cannot be recovered—it is not clear that the operators would benefit from rushing to adopt terrestrial wireless technologies before their current satellites reach end of life.

Second, startup satellite operators focused on IoT have taken a mixed approach to terrestrial wireless technologies. Some, like Astrocast of Switzerland, Canada’s Kepler Communications, French IoT connectivity provider Kineis, Australia’s Myriota, British-based Sky and Space Global, and Swarm Technologies in California, follow the traditional approach of using

Cumulative Global Satellite IoT Connections, By Region, 2019-2025



Source: Omdia 2020.

proprietary connectivity technologies. Others, such as Fleet, Ligado, Dutch-based Hiber, the UK's Lacuna Space, OQ Technology of Luxembourg, and Silicon Valley's Skylo Technologies use terrestrial wireless protocols, but sometimes in conjunction with terrestrial gateways. For example, Fleet uses LoRaWAN to connect 1,000 devices to a local gateway, but the gateway uses a proprietary, non-terrestrial technology to connect to Fleet's satellites.

Third, connecting end-devices directly to satellites using terrestrial wireless technologies is complex and requires an investment in research and development. Fleet makes no attempt at all to undertake such an operation, using LoRaWAN only as a terrestrial technology. For Hiber, its directly connected LoRaWAN devices communicate only in the uplink direction because of interference concerns with the amount of power that Hiber satellites would need to communicate on the downlink in unlicensed ISM band spectrum. Ligado can now support NB-IoT and LTE-M now, benefitting from a massive 22-meter antenna on its GEO satellite, and is working with Ericsson and Sequans on 5G. OQ Technology, meanwhile, is still testing its approach. And Skylo Technologies—technically a reseller but possessing noteworthy intellectual property—claims to have an interesting proprietary approach that utilizes NB-IoT in conjunction with third-party GEO satellites; the company has raised $116 million in venture funding.

Because of the variety of proprietary approaches that exist in using mobile terrestrial technologies for satellite connectivity, the 3GPP standards body that develops protocols for mobile telephony should ensure that the 5G standard addresses connectivity to satellites and other non-terrestrial networks, such as unmanned aerial vehicles. However, support for satellite components in 5G architecture, which should be available with 3GPP Release 17, is not slated to be finalized until September 2021.

Recommendations

Given the overall picture, Omdia believes that terrestrial wireless technologies will have a long-term, 10- to 15-year-horizon impact on the satellite IoT industry. But owing to technical constraints, such as distance and Doppler shifting, line-of-sight requirements, as well as additional service costs to roam onto the satellite network, satellite will likely never replace terrestrial networks as the first-choice connectivity option for IoT. Nevertheless, we expect that within a 15-year to 20-year time horizon, the distinction between a "satellite IoT" device and a "terrestrial IoT" device will cease, and any device with embedded mobile connectivity will be capable of roaming onto satellite networks when out of range of terrestrial infrastructure.

The distinction will disappear because as the 3GPP works to make 5G—and future "Gs"—compatible with non-terrestrial networks, no net additional device hardware cost will be incurred for a mobile device to roam onto a satellite network when terrestrial networks are unavailable. For many IoT applications, having the ability to roam onto satellite networks when needed will be attractive. Overall, this should shift the satellite industry toward 5G—and beyond—to enable such a backup option for satellite customers, which means that even "satellite-first" IoT connections will increasingly utilize terrestrial wireless technologies.

Ultimately, most stakeholders will treat satellite connectivity as simply another means of getting remote data into cloud-based IoT applications. In contexts where data may have been previously unavailable because the device was out of range of a terrestrial network, it will act as an IoT market growth driver. For mobile network operators specifically, an important opportunity will be available to leverage roaming partnerships with satellite operators and expand the addressable market for their core IoT connectivity propositions.

“The Internet of Things (IoT) has already conquered the earth, with billions of devices everywhere—from cars, to factories, to entire cities. Now the IoT is blasting off into space, with cumulative satellite connections expected to rise to more than 10 million by 2025.”

The road to opportunity is paved with connected cars

John Canali
Senior Analyst, IoT

During the next decade, the light vehicle and commercial automotive space is expected to become home to 6.5 billion connected IoT devices, offering enormous opportunities for original equipment manufacturers (OEMs), communications service providers (CSPs), systems integrators, hardware/software developers, and a host of other technology players.

The global installed base of connected devices in these vehicles is expanding rapidly, growing by nearly a factor of six from 1.2 billion in 2020. As the industry moves toward autonomous vehicles, new growth opportunities are emerging. At the same time, the market landscape is becoming more convoluted, involving regulators, standards bodies, and city and transportation planners.

With the market expanding and the ecosystem widening, the connected car value chain is shifting. However, OEMs remain at the center of it all.

OEMs have been making new investments and developing partnerships around the technologies needed to enable and secure autonomous driving. They are also taking strategic steps to gain greater ownership of the evolving connected and autonomous vehicle value chain.

A complex ecosystem and a highly contested market

The connected car ecosystem is expanding in terms of both new services and new players, as shown in the figure below. As vehicles become more autonomous, complementary technologies such as autonomous driving software, artificial intelligence, cloud management, and data analytics will create new opportunities for players with greater expertise in these areas than automotive manufacturers. Internet companies and cloud players like Amazon and Microsoft can expect strong future growth in the automotive vertical, while the expanding ecosystem will also open the door to startups around autonomous enablers such as Argo.AI and Cruise Automation.

Autonomous cars reshape the automotive competitive landscape

While the ecosystem and market are expanding, not all players will benefit equally.

Traditional telematics service providers (TSPs) will struggle as OEMs look to bring their telematics platforms in-house. While connectivity will become an ever-more critical enabler of connected vehicles, CSPs will face more intense competition from one another, as well as from newer global connectivity providers such as Ireland’s Cubic Telecom, "As the industry moves toward autonomous vehicles, new growth opportunities are emerging. At the same time, the market landscape is becoming more convoluted, involving regulators, standards bodies, and city and transportation planners."

Tata Communications of India, and French-based Transatel. Systems integrators should see opportunities in the short-term that enable them to provide strategic guidance around best practices.

Major cloud and internet leaders such as Google and Amazon are well-positioned to expand their role in autonomous vehicles, leveraging their cloud and data expertise as cars generate—and require—ever-greater amounts of data to understand driver behavior and physically map the roads. Moreover, some are aggressively investing in autonomous driving technologies. For their part, enterprise software vendors are going to find new opportunities, especially those related to applications for data management, analytics, and integration.

The expanding market has also attracted many startups, even though most connected automotive startups have had little success to date, with Tesla being the only exception.

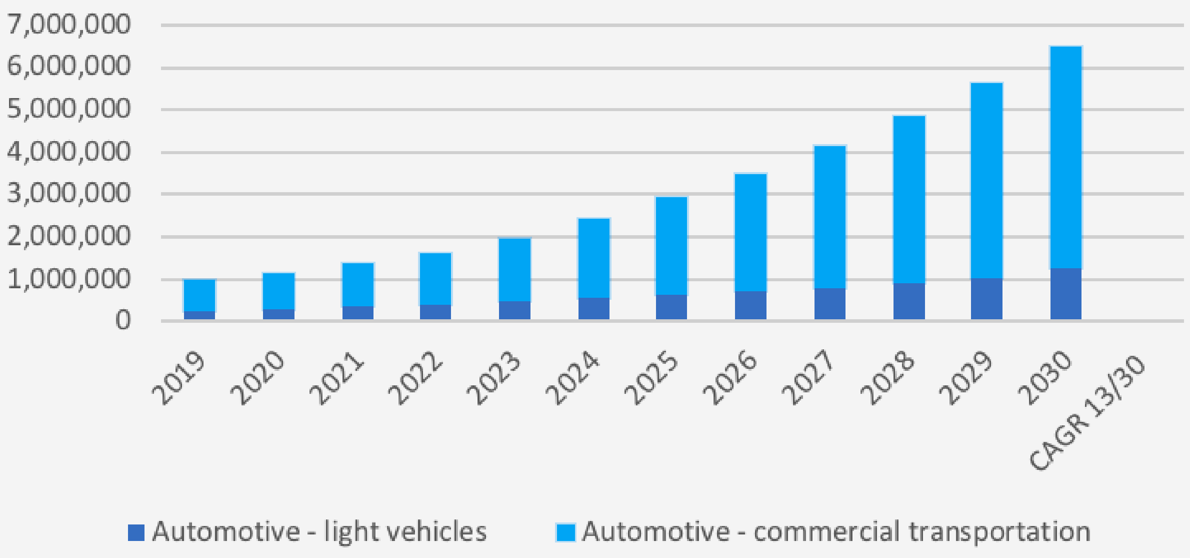
OEMs make connected-car power play

Automotive OEMs are positioning themselves to ensure that they maximize control over the value chain. Many major OEMs are making investments to bring as much as they can of the connected-car technology stack in-house. As a result, OEMs are creating proprietary telematics platforms, developing their own insurance and mobility services, and making large investments in companies that focus on autonomous driving.

In 2016, GM spent more than $1 billion to acquire a majority stake in Cruise. The company has since attracted large investments from Honda, Softbank, and T. Rowe Price, and has since been valued at $19 billion. Ford and Volkswagen have each made commitments of over $1 billion to Argo.AI. These moves are a departure from the traditional notion in which OEMs see other players in the value chain largely as suppliers and not partners, with each player having its own niche and the OEM then designating the role it believes is appropriate for each player.

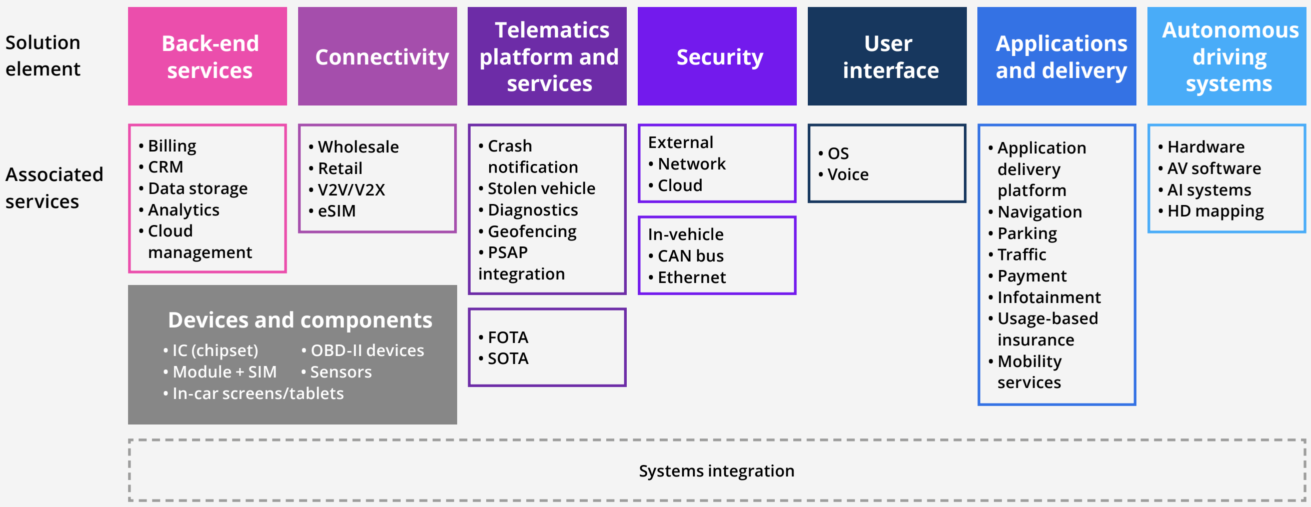
But just because OEMs are seeking greater control over the connected car solution does not ensure that they will succeed, nor does it imply that they take is the optimal strategy for them. In fact, the reverse is true: The growing complexity of technologies and the overall ecosystem in the road to autonomy will require OEMs to work more in partnership with other market players. Such a move is critical if OEMs wish to successfully leverage the new opportunities around connected car data and to bring new offers to market in a timely and economically viable fashion.

Global installed base of internet-connectable devices in automobiles (thousands)



Source: Omdia 2020.

Connected car solutions value chain



Solution element	Back-end services	Connectivity	Telematics platform and services	Security	User interface	Applications and delivery	Autonomous driving systems
Associated services	• Billing • CRM • Data storage • Analytics • Cloud management	• Wholesale • Retail • V2V/V2X • eSIM	• Crash notification • Stolen vehicle • Diagnostics • Geofencing • PSAP integration • FOTA • SOTA	External • Network • Cloud In-vehicle • CAN bus • Ethernet	• OS • Voice	• Application delivery platform • Navigation • Parking • Traffic • Payment • Infotainment • Usage-based insurance • Mobility services	• Hardware • AV software • AI systems • HD mapping

Devices and components
- IC (chipset)
- Module + SIM
- In-car screens/tablets
- OBD-II devices
- Sensors

Systems integration

Source: Omdia 2020.

Furthermore, the automotive market is at a major inflection point, with connectivity and autonomy being major trends, alongside electrification and the advanced human-machine interface (HMI). Not only must OEMs make major investments and bets in all these areas, they must also rely more heavily on suppliers and partners.

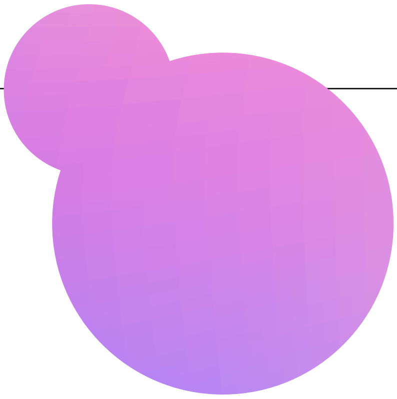
Recommendations for technology players and service providers

With the emergence of technologies such as 5G and AI, there are opportunities for technology players and service providers to expand or enhance their roles in the connected car value chain. This must be done within ecosystems that include the OEMs and not conducted in isolation. As cellular vehicle-to-infrastructure (CV2X) becomes a global standard for communication between increasingly autonomous cars and the built environment, OEMs will need to work with CSPs, system integrators, cellular infrastructure providers, and regulators, to ensure that systems are safe and reliable. OEMs will also need to work increasingly with CSPs on network rollout planning.

The 5G rollout is a good time for CSPs to reassert their role as crucial partners in the connected car ecosystem, especially since OEMs have benefited from CSP competition. Because automotive connections can have a retail component in the form of Wi-Fi and content, OEMs will often demand extremely low wholesale connectivity rates, in exchange for providing the CSP with the chance to pursue retail opportunities for in-car services.

In the end, 5G could prove to be a key differentiator for some CSPs. OEMs that wish to establish themselves as leaders in autonomous driving will need to partner with the CSPs that have the most robust networks. For their part, CSPs should leverage their 5G strength to shift relationships with OEMs toward more of a partnership than that of being a pure supplier.

Smart cities offer a $44 billion opportunity for IoT providers, but monetization remains challenging



Carrie Pawsey
Senior Analyst, IoT

Omdia forecasts a $44 billion opportunity by 2023 for IoT technology providers with an installed base of 400 million devices. However, progress to date has been slow and steady, because the vertical is highly fragmented, and monetization remains challenging.

Omdia has identified three smart city strategic approaches being adopted by cities across the world: the point solution city, the city brain, and the holistic city. Finance plays a key role in determining which strategy a city can choose and how quickly services are rolled out. Monetary issues also govern the level of integration for a smart city's services, determining whether they operate in a converged way or in a more siloed manner.

Most cities start with a point solution approach, based on multiple individual services that are largely financed by local government budgets. Business cases tend to be built around a single application, which results in a patchwork and siloed approach. Some cities are now evolving to the city brain approach, where a single platform is deployed to collect and analyze data across multiple smart city applications. However, financing for the city brain is more complex and requires funding innovation beyond local government budgets.

Smart cities using holistic approaches are usually greenfield cities, often found in Asia or the Middle East. In some cases, these are very large cities that are being built from the ground up. In more developed countries, "smart districts" are more commonly seen being built on brownfield sites. Holistic cities, meanwhile, require very large amounts of public funding together with private investment, and are often part of a wider national digitalization and transformation strategy.

Financing is a key challenge for cities both in terms of securing funds and finding the right long-term sustainable business model. A mix of public and private funding is required for long-term viability. The underlying business models must allow the technology providers to monetize the city but also allow cities to achieve their non-financial goals around sustainability and resilience, as well as improving citizen's lives.

The three smart city strategic approaches

Each of the three smart city approaches has its own benefits and challenges. These approaches are typically associated with different funding models, and they also have different implications for vendors looking for entry points to smart cities partnerships and contracts.

1 The point solution city

Most cities take the point solution approach, at least at the start of their digitization journey. Projects are deployed on a single-use-case basis and are usually driven by governance, planning cycles, and an inability to move beyond the immediate use case. Projects are largely funded by local government budgets as part of their procurement process, or through test-bed trials involving start-ups, academic bodies, or smaller private companies either for private funding or in public-private partnerships.

While this is the most common smart cities approach, very often projects struggle to move beyond the proof-of-concept (PoC) stage, or fail to scale up, or both. The biggest issue for point solution cities is the silos of data that are the result of a fragmented project approach, with multiple vendors using several technologies.

Technology providers looking to monetize point solutions cities should target local authority departments as part of their procurement processes; or work with public service contractors, such as waste management companies or parking providers, to digitalize their businesses and help win contracts from the cities.

2 The city brain

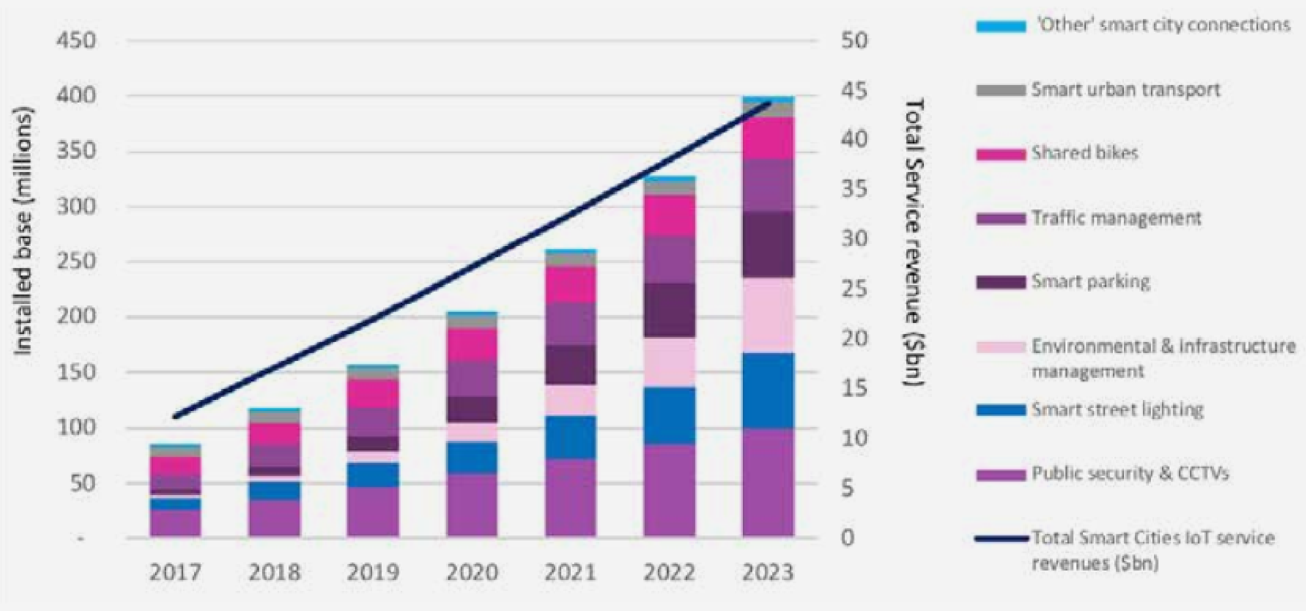
The city brain is the result of an evolution strategy that sees cities move from a point solution into the next phase, overlaying analytics to converge the different data sets and creating a single "city brain" as a result. The objective is to retrospectively break the silos and knit together all the city data in a single platform or in multiple interoperable platforms. This requires additional investment beyond the usual local government budgets.

These cities are usually further along their smart journey and have a smart city team looking to deliver a holistic smart vision, although rollouts to date may have been conducted in a patchwork way based on single-use cases. Smart city teams encompass many different job titles and roles, including—but not limited to—chief data officer (CDO), chief information officer (CIO), smart commissioner, city digital strategist, innovation hub team, and smart city project manager. Some of these roles are funded by local government; others are paid for by private funding through multiple project business cases.

Omdia also sees vendor financing playing a role in enabling the city brain, because building a business case for a single platform where point solutions have already been deployed is challenging. Technology providers should be selling into these smart city teams and working with them to find innovative funding for more holistic-focused projects.

> "Omdia has identified three smart city strategies being adopted by cities across the world: the point solution city, the city brain, and the holistic city. Finance plays a key role in determining which strategy a city can choose and how quickly services are rolled out."

Smart Cities installed base and revenues



Source: Omdia 2020.

3 The holistic smart city

Holistic smart cities are usually greenfield cities establishing digital infrastructure for the first time or undertaking a complete overhaul of their legacy infrastructure, often as part of a brownfield district regeneration program. Holistic cities have a single smart city vision with a clear integrated roadmap from the outset.

This “big bang” approach requires dedicated and large amounts of financial backing from the central government together with additional private funding. Technology providers looking to monetize holistic cities should recognize that these are often big projects with long timescales. These projects involve large tenders, and contracts are often awarded many years in advance. Budgets for such projects are often managed by a federal ministry body rather than by local authorities.

Technology providers should look to partner with large, well-known systems integrators or local incumbent information and communication technology (ICT) providers, because these are usually the prime contractors and will often bring smaller partners on board.

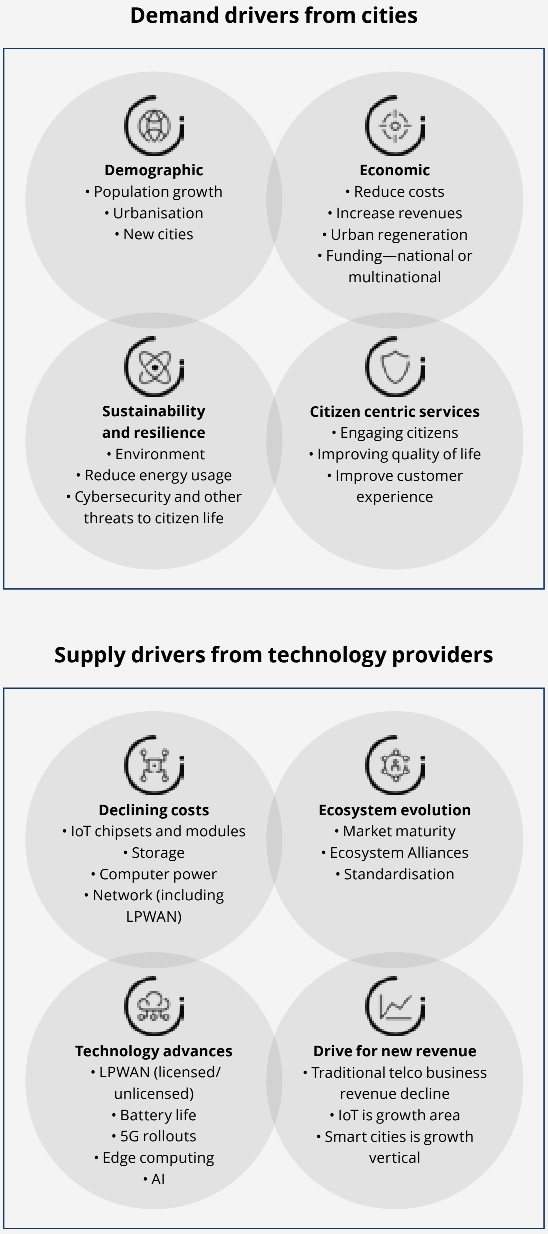
Recommendations for smart city funding and strategies

Smart city monetization remains a challenge and scaling smart city solutions beyond the pilot phase is difficult for all cities. Funding smart city development is a key challenge for cities in terms of both securing upfront investment and finding the right long-term sustainable business model. A mix of public and private funding is required for long-term viability.

Cities and their suppliers need to be innovative in approaches to financing and business models. Smart city business cases should look beyond cost savings and local government funding. A city brain approach, for example, could allow the city to turn data into a key asset, although compliance with data privacy regulations must always be part of the thinking for such initiatives. Suppliers not only need to help cities identify grants and funding where possible, but more importantly work with them to help create public-private partnerships (PPPs), which are key to the longevity of smart city projects.

To seize the projected $44 billion opportunity in smart cities, IoT technology providers need to understand a city’s strategic approach to apprehend and recognize which entities hold buying power. For point solutions, the entities usually are the local government departments, while for holistic cities they are often the larger ministerial bodies. City brain approaches often entail a longer-term view and some creative financing, and suppliers need to identify stakeholders carefully, helping cities build a compelling business case with a clear return on investment.

Supply & demand drivers for smart cities



Demand drivers from cities

Demographic
- Population growth
- Urbanisation
- New cities

Economic
- Reduce costs
- Increase revenues
- Urban regeneration
- Funding—national or multinational

Sustainability and resilience
- Environment
- Reduce energy usage
- Cybersecurity and other threats to citizen life

Citizen centric services
- Engaging citizens
- Improving quality of life
- Improve customer experience

Supply drivers from technology providers

Declining costs
- IoT chipsets and modules
- Storage
- Computer power
- Network (including LPWAN)

Ecosystem evolution
- Market maturity
- Ecosystem Alliances
- Standardisation

Technology advances
- LPWAN (licensed/ unlicensed)
- Battery life
- 5G rollouts
- Edge computing
- AI

Drive for new revenue
- Traditional telco business revenue decline
- IoT is growth area
- Smart cities is growth vertical

Source: Omdia 2020.

Tech leaders join forces to resolve smart home interoperability challenges

Lee Ratliff
Senior Principal Analyst, IoT & Connectivity

Mariana Zamoszczyk
Senior Analyst, Consumer Services

In just one decade, the global installed base of connected home appliances and home automation devices will soar to 24.8 billion units, up from 712 million in 2020—a massive number of IoT devices that will spur an equally massive interoperability challenge, according to Omdia.

To solve the interoperability issues that are constraining growth in the smart home market, top technology players are joining forces. In December 2019, a consortium including Amazon, Apple, Google, and the Zigbee Alliance announced the formation of a new working group to address application-layer interoperability in the smart home. The Connected Home over IP (CHIP) project will operate as a working group under the auspices of the Zigbee Alliance, borrowing the Alliance's organization and infrastructure.

A CHIP off the old block

CHIP's goal is to create an application-layer interoperability protocol built on top of existing native-IP connectivity standards such as Wi-Fi, Bluetooth, and Thread. Omdia believes this is a positive and essential step for the smart home market as it attempts to cross over from the early adopter demographic to the mainstream consumer market.

While what the final standard will look like is unknown, Omdia's hope is that CHIP will enable OEMs to easily make products that work in every major ecosystem and that consumers need not be concerned about interoperability when making purchases. It is even possible that CHIP may blur the lines among ecosystems to such a degree that they become unimportant. Devices will not just work; they will work together across ecosystem boundaries.

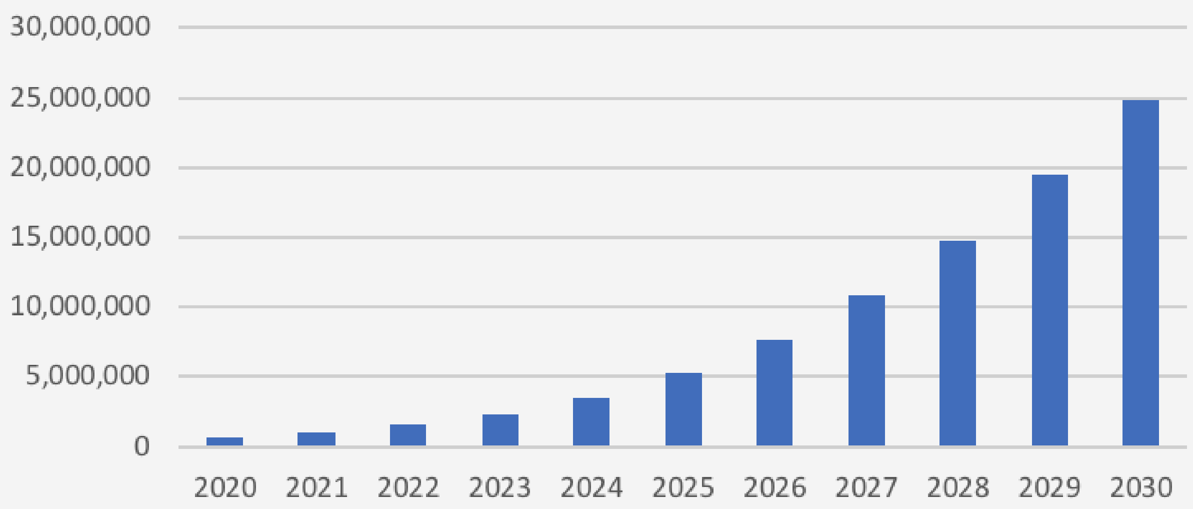
The value bestowed by achieving interoperability cannot be overstated. In the coming years, the market for connected home appliances and automation device shipments will exceed 2 trillion.

Democracy in action

The structure of CHIP is surprisingly democratic. The group will borrow its structure from the Zigbee Alliance, a neutral party. Each member company will have one vote on CHIP decisions, which means Amazon, Apple, and Google will each have one vote—the same as that held by the smaller companies involved in the working group.

While Omdia expects the three headline companies to have outsized influence, they will not be able to dictate CHIP

Worldwide installed base for internet-connectable devices for home appliances home automation (Thousands of units)



Source: Omdia 2020.

decisions through voting, ensuring that smaller companies are heard. We have been told that Amazon, Apple, and Google are sensitive to the perception that the three giants working together could be seen as an effort to collude on market outcomes, a form of price fixing. To forestall such a view from emerging at the outset, CHIP has been structured to be as open, inclusive, and democratic as possible.

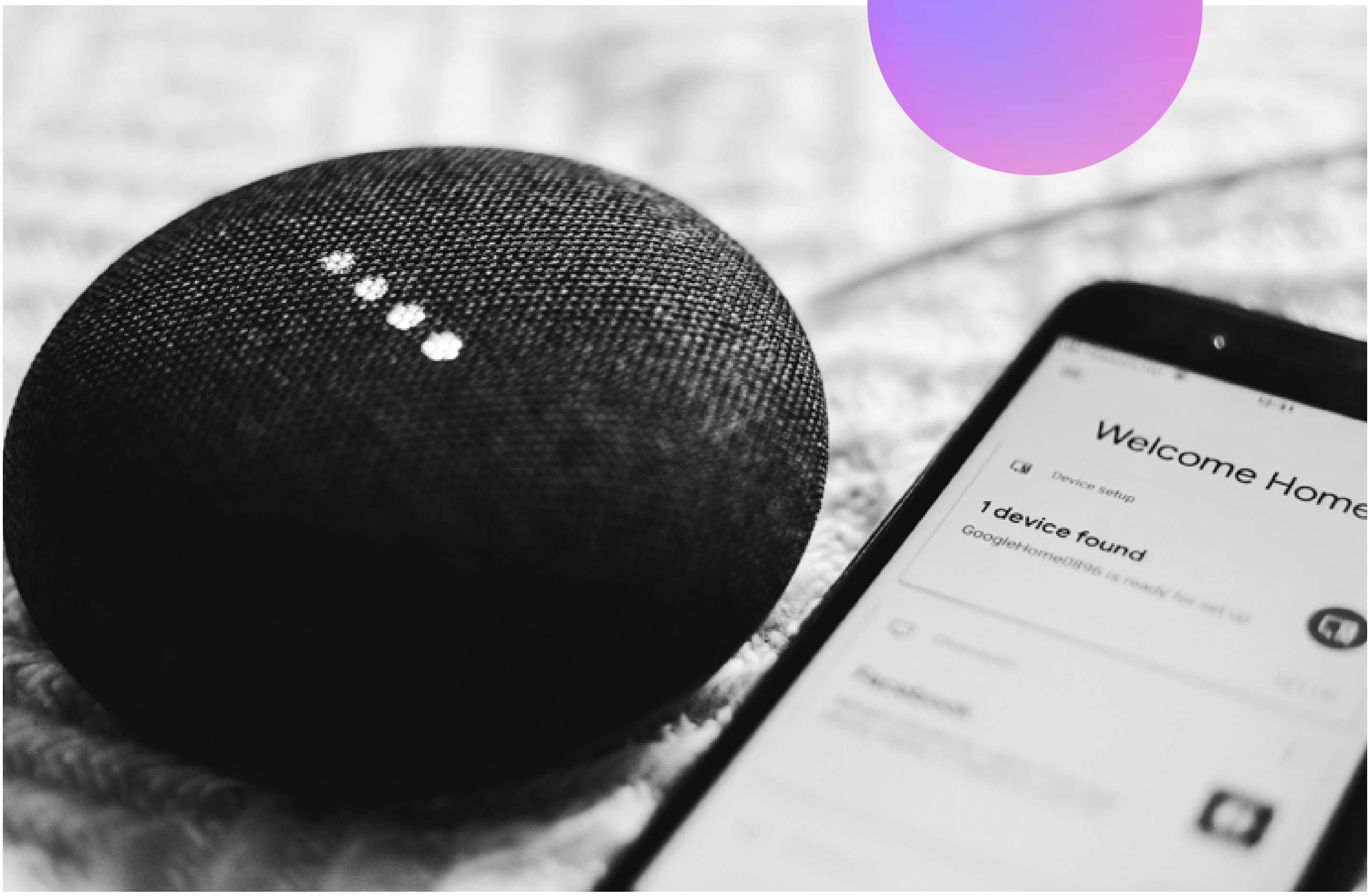
Will things get chipper at CHIP?

One point of potential disagreement within CHIP strikes at the very premise of the group: the use of end-to-end internet protocol (IP) within the smart home. IP is a simple, yet powerful, transport layer that could tie together smart home ecosystems with existing mobile and IT ecosystems that already use IP. The use of IP enables the reuse of assets from other markets, including code, applications, developers, tools, and semiconductors. Having participated in the mobile and IT markets prior to entering the smart home space, Amazon, Apple, and Google are all very comfortable with IP and hope to leverage their prior work as much as possible in developing platforms and solutions for the smart home.

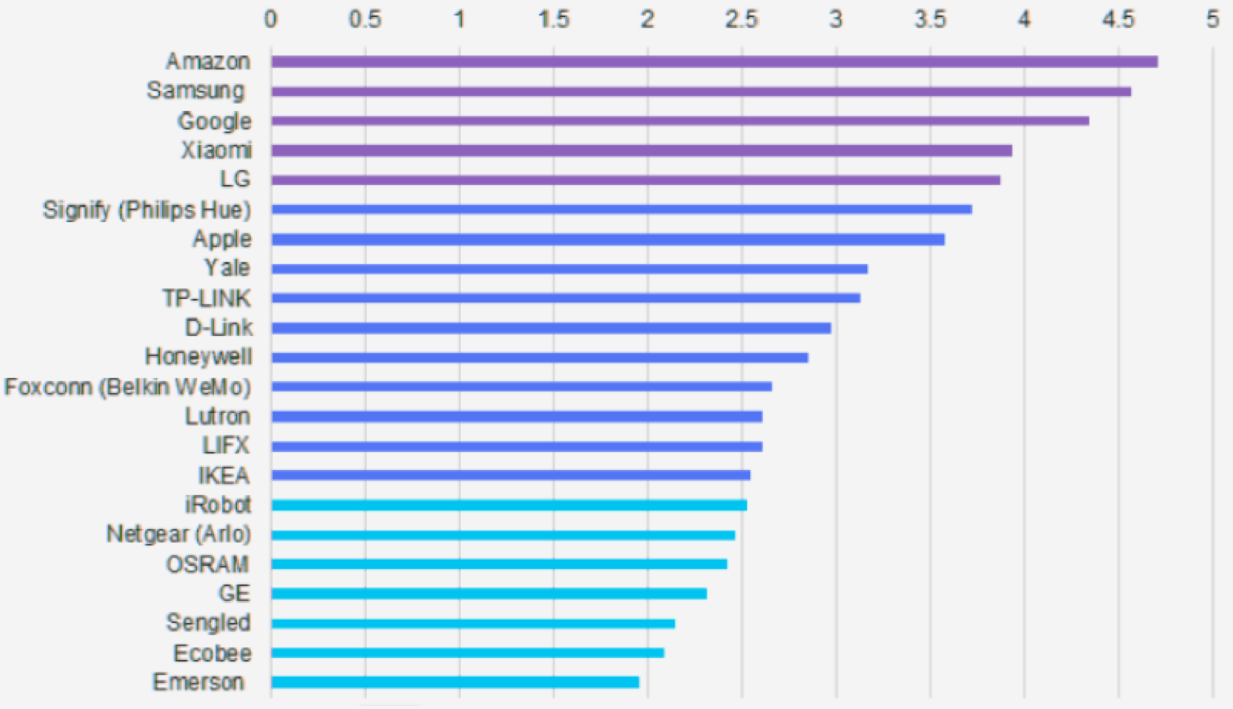
However, while legacy smart home OEMs seem to be generally in favor of IP for the backbone and branches of the smart home network, many of them want some flexibility on choosing the most appropriate connectivity for the last hop to the end node. This is especially true in the case of cost-constrained devices and cases wherein backward compatibility with legacy devices is critical. For the most cost-constrained devices, such as temperature sensors, the overhead of IP might mean transmitting hundreds of header bytes when the payload is only a few bytes of data. The effect on the most cost-constrained devices will be increased complexity, rising hardware requirements, and expanding on-air time, driving up price and power consumption. In addition, companies like Signify, makers of the Philips Hue smart lighting solutions, have large installed bases of legacy devices using non-IP connectivity solutions such as Zigbee. Requiring IP support could cause interoperability problems for legacy customers.

While the CHIP effort faces numerous technical and political challenges that must be negotiated and resolved, Omdia believes the effort is a necessary step for the smart home market. Like any standards effort, CHIP will ultimately represent a compromise solution and may fall short of initial expectations. However, the willingness of the top three industry players to work together is a highly positive sign for the future of the smart home.

“Omdia’s hope is that CHIP will enable OEMs to easily make products that work in every major ecosystem and that consumers need not be concerned about interoperability when making purchases. It is even possible that CHIP may blur the lines among ecosystems to such a degree that they become unimportant. Devices will not just work; they will work together across ecosystem boundaries.”



Smart home vendor benchmark – 4Q 2019 scores



Source: Omdia (Ovum) Smart Home Vendor Benchmark, 2019

Note: Vendors are scored from 1 (lowest) to 5 (highest) on five different elements of smart home leadership: business model, technology and innovation, reach and impact, ecosystem, and user experience.

Key: Green = Leader; Yellow = Challenger: Red = Follower.

Recommendations for smart home players

- Semiconductor vendors seeking to participate in the smart home market should ensure the inclusion in their wireless product portfolio of one or more technologies that support IP transport. Chief among these are Wi-Fi, Bluetooth Low Energy (BLE), and Thread. Participation in the CHIP working groups is advised, so that vendors can accurately anticipate product requirements, influence specifications, and achieve quick time-to-market. Semiconductor vendors may also wish to develop their own CHIP stack or participate in an open-source initiative to ensure they have the software tools necessary to sell their hardware products.

- Smart-home-device and solutions vendors should ensure the new protocol is not disruptive for customers, especially those owning legacy smart home devices. Limited compatibility among devices has been a major bottleneck in the smart home. The willingness of vendors to work together to solve this problem is good news, but participants should be careful not to confuse the larger issue at hand, with issues relating to customers that do not really understand or care about connectivity protocols but simply desire a frustration-free set-up process and to know that their devices are safe.

- For CHIP to be successful, smart home vendors need the entire ecosystem to be on board. This means not only convincing market participants that this is the correct approach and strategy for moving forward, but also making sure that support—in the form of tools, funding, and incentives—is adequately provided.

Manufacturers need new approach to overcome industrial IoT deployment hurdles

Alex West
Senior Principal Analyst,
Industrial Technology

Not since electrification has the industrial sector seen anything as potentially transformative—or hyped—as digital transformation. The promises of digital transformation are alluring to industrial execs, offering the potential for solutions that can impact business across the entire life cycle of production—from faster, more flexible and efficient design, through to the introduction of new after-sale services that can forge stronger relationships between manufacturers and suppliers.

In the manufacturing sector, the Industrial Internet of Things (IIoT) is a critical element of digital transformation, with global shipments of IIoT devices set to rise to 129 million units in 2023, up from 85 million in 2020. While this all sounds great, concrete adoption of advanced digital solutions in the industrial market is still very much limited to the innovators. Most companies are not yet trialing IIoT projects or are hosting stalled proof-of-concept (PoC) projects. Actual deployments, meanwhile, have not delivered expected value.

Why is deploying the IIoT so difficult?

IIoT value must align with business needs

All over industry, manufacturing customers and their information technology (IT) and operational technology (OT) teams alike are being confronted with a slew of digital technologies and solutions, a formidable array that may include the cloud, artificial intelligence, robotics, augmented and virtual reality, additive manufacturing, and digital twins. All promise a revolution in how products are manufactured.

Ultimately, however, the success or failure of these technologies in the manufacturing sector will depend on their capability to address the pain points that manufacturers face today. Common challenges within the industrial sector include:

- Coping with an aging workforce and difficulties in recruitment
- Improving productivity and reducing unplanned downtime
- Flexibility and speed to market
- Driving sustainability, a more recent—but increasingly compelling—requirement

> "Concrete adoption of advanced digital solutions in the industrial market is still very much limited to the innovators. Most companies are not yet trialing IIoT projects or are hosting stalled proof-of-concept projects. Actual deployments, meanwhile, have not delivered expected value."

Aligning IIoT solutions with these business problems is crucial for ensuring project funding, executive support, and successful adoption by businesses in the sector.

Omdia tracks case studies of outcomes resulting from the adoption of IoT and digital solutions in the manufacturing sector. Some examples of innovators that have started to see value for their business include:

- Cargill Inc., which achieved a **40% cost savings in manpower** by relying on a centralized team of five analysts to support the condition monitoring of 15,000 machines
- Jabil, which improved its quality management systems, resulting in savings exceeding 15% in **scrap and rework costs,** as well as an additional 10% reduction in **energy costs**.
- Siemens, which reduced its **time to market** and **lead time** for some products while increasing its **flexibility in product design and adjustments**.
- Baker Hughes, which earned a $101 million annual reduction in **unplanned production losses** while seeing an increase in its electric submersible pump (ESP) run-life, with 66% of failures predicted 60 days ahead of the failure date.

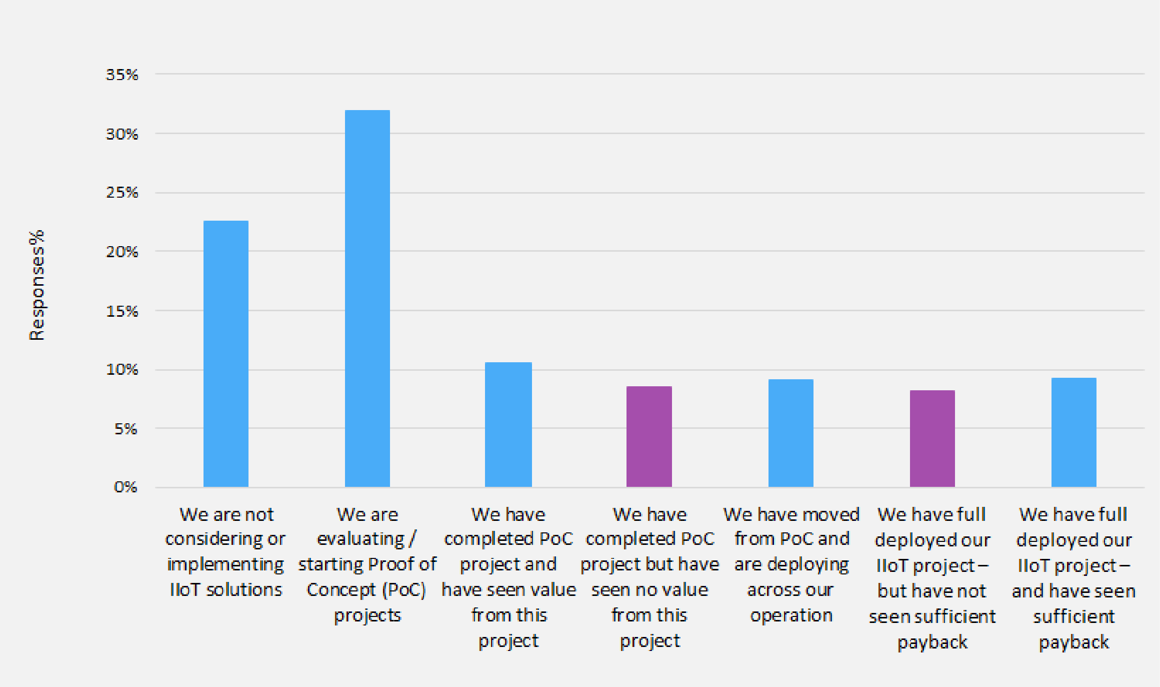
Deployment challenges

While these innovators are seeing strong results from IoT adoption, many in the manufacturing and industrial sectors continue to struggle with digital transformation. And among those that have begun trials, the results have been decidedly mixed.

According to a recent Omdia survey of manufacturing enterprises, 54% of manufacturers have not yet implemented any type of IIoT project, whether at PoC or deployment. Just under half report their PoC having failed, which is acceptable for companies attempting to be agile and trial new applications. However, a similar "failure" rate—defined by companies as not seeing enough return on investment—is reported when companies move to the deployment stage, meaning that companies are investing in IIoT projects but are not getting the payback they expected.

Some of these results can be attributed to inflated expectations of a quick payback. Half of companies Omdia surveyed reported that they had expected to obtain payback within one year, a very aggressive target. While there are always exceptions, Omdia expects many of these projects

At what stage of maturity are IIoT project?



Source: Omdia 2020. (2018 Enterprise Survey)

to take much longer to generate returns, often extending to two to three years.

Beyond the unreasonable expectations, companies looking to deploy IIoT solutions face a plethora of other challenges, including:

- **Legacy equipment and infrastructure**
  The industry must contend with retrofitting and upgrading existing equipment as well as brownfield facilities to enable a connected factory. while the worldwide installed base of industrial machines numbers more than 220 million, Omdia estimates less than 10% of these are IIoT enabled.

- **Cybersecurity**
  Over half of manufacturing companies have experienced a cybersecurity breach during the last three years, yet investment in cybersecurity is still not a major investment focus for most companies.

- **Collecting and deriving meaning from data**
  As IIoT-related technologies are introduced, the volume, variety, and velocity of data can increase exponentially. Many companies stumble in moving from just having data, to generating actionable information.

As if the above concerns aren't already daunting, there are yet more challenges related to organizational change, interoperability, and investment. However, Omdia believes the single most significant pitfall is not directly related to technology. Instead, the problem has to do with people, on issues such as:

- Training the workforce to trust and utilize new solutions

- Upskilling workers for them to possess the necessary IIoT skill sets

- Obtaining buy-in, especially from middle management, and ensuring that IIoT solutions are not seen as a threat to job security

Steps to IIoT success

Manufacturing enterprise end-users and their technology partners would do well to carefully consider six important elements—or the six s's—in any IIoT implementation:

- **Specify**
  As with any project, it is important to identify the problem or pain point that the technology aims to fix, not the other way around. Successful IIoT projects start with a clearly defined objective at the outset.
- **Success**
  Define success or establish a point of reference that will be used to measure success. The insights gained from this benchmark will show what worked, what didn't, and how things could be improved.
- **Start small**
  Begin IIoT implementation by initiating pilot projects or proof-of-concept cases to determine how the technology works and where the value lies for the business. Companies may then move to deployment and scale accordingly once these crucial steps take off.
- **Senior-level support**
  Obtain buy-in from senior-level management not only for funding purposes but also for dealing with the inertia that arises within the organization. Implementing any big changes, especially those as radical and sweeping brought about by IIoT, are likely to meet with resistance.
- **Shared responsibility**
  Enabling convergence among different functional teams is crucial, given that IIoT projects require substantial time, effort, and resources. And with different teams within the same organization possessing varying goals and responsibilities, organizations must strategically align the twin aspects of IT and OT—information technology and operations technology—within the enterprise to resolve conflict and harmonize implementation.
- **Support the people**
  The most important determinant of IIoT success is the people within the organization who will be using IIoT. Acceptance and trust from employees that the technology will not take away their livelihood will be key to successful IIoT deployment. This can be achieved by creating awareness, as well as by educating and providing employees with training to expand their skill sets.

Proliferation of devices results in propagation of cyberthreats for Industrial IoT

Tanner Johnson
Senior Analyst,
Cybersecurity & IoT

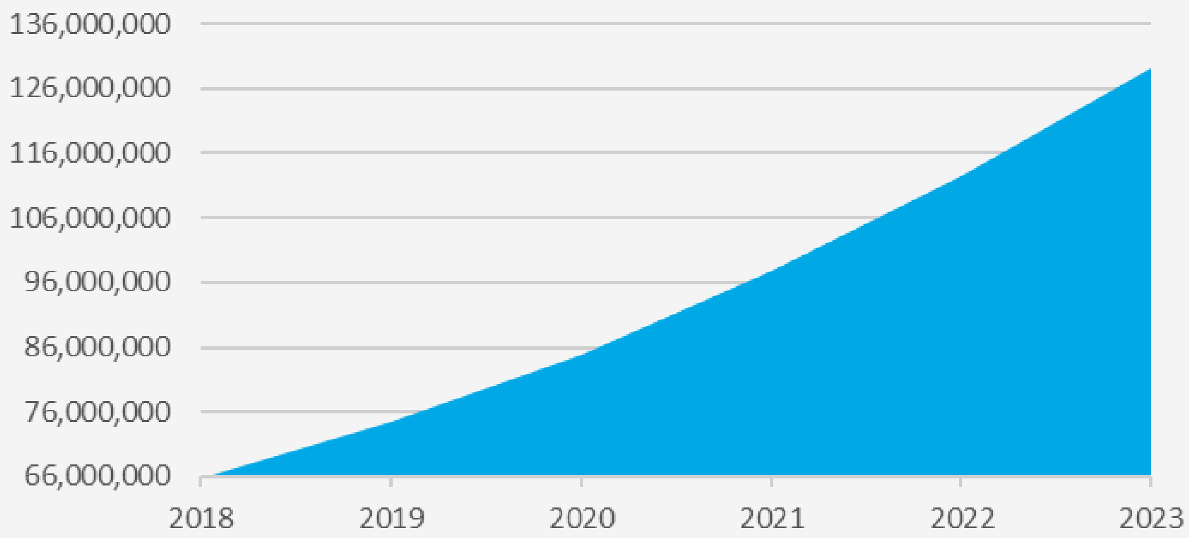
The explosion in shipments of Industrial IoT (IIoT) devices has been accompanied by a proportionate increase in cyberthreats, as the devices present new attack vectors for hackers to breach and infiltrate, according to Omdia.

Cyberattacks are of particular concern in the industrial sector, where unit shipments of IIoT devices will grow by 52% percent in just the next three years. Given the massive base of potentially vulnerable devices involved, we now find critical infrastructure and industrial networks routinely ensnared in the crosshairs of potential cyber-criminals and data thieves.

As the use of connected devices in these settings grows, IIoT deployments remain a consistent target because of several characteristics unique to critical infrastructure and industry, including:

- The overall age of underlying legacy components of critical infrastructure, which poses a unique security challenge
- The increased demands for consistent, uninterrupted operation of legacy systems that comprise the infrastructure
- Given the absence of any fully developed and mature security standards, much critical infrastructure is run on a diverse range of makeshift solutions consisting of an assortment of hardware and software products, which present security concerns owing to their unique configurations
- The sheer volume of IoT devices being placed inside industrial facilities due to the increasing demand for equipment monitoring and management, creating an enormous attack surface to target

Global IIoT device unit shipments



Source: Omdia 2020.

Aging legacy systems pose a unique challenge

Much the world's critical and industrial infrastructure currently operates on outdated hardware components and obsolete software configurations. And because security was not organically built into the development of these legacy systems, they are rife today with vulnerabilities that may be exploited through increased connectivity.

Regrettably, simply being aware of various vulnerabilities present in aging infrastructure doesn't necessarily translate into solutions that are easy to implement. These systems are typically not maintained or updated with security patches, even if vulnerabilities are well-known. As the organizational environment of each facility is unique and entirely dependent on the specific demands of its own industry, this often results in the adoption of customized hardware and software configurations to meet the requirements of explicit operational tasks. As a result, developing an established update or patch management system can be daunting, especially if the proposed updates result in other components of the facility failing to work properly afterward.

While the isolated nature of operational technology (OT) functions and systems historically added a layer of protection, many long-standing OT practices have now become security liabilities. Limiting access to physical connections made practical sense when the only devices that needed to connect to the network were hardwired authorized components and machinery necessary to perform specific functions and tasks. However, as demand for greater access to operational analytics grew, more legacy components needed retrofitting with more advanced IoT devices and sensors. Those needs continue today, with newly installed devices requiring network access to report any captured data.

Increased demand for uninterrupted access to IIoT devices

Despite vulnerabilities and the introduction of more points of compromise into the environment, consumer demand for consistent reliability and output from critical infrastructure can supersede any effort to secure the systems. There is always a risk that any security update or patch management system may inadvertently lead to an interruption in service, which can produce catastrophic results, affecting both the operational safety and financial stability of a facility. This combination of dependency and vulnerability adds to the challenge of securing IIoT deployments.

Moreover, industrial facilities face enormous challenges in their effort to transition mission-critical communication infrastructure to digital and automated operations. Such a mandate—along with the growing demand for operational and infrastructure data—requires that these systems be methodically updated with capabilities that allow for effective monitoring and management. If not implemented properly, however, the transition to automation and software-controlled production can create even more security risks and potential operational disruptions.

Lack of standards and diversity of protocols hamper efforts

The growing need for IIoT security is prompting many industrial IT managers to look for a standards-based approach to both IoT technology and IoT cybersecurity. Standards developed for general IT security do not easily transition over to operational technology (OT) and have not been adopted consistently. Some standards are simply unenforceable within the OT environment, owing to the diversity of each industrial setting.

The diversity and lack of standardization of IoT communications protocols are also barriers, leaving industrial IT managers to be faced with multiple options for short- and long-range wireless and fixed connectivity solutions. Here the choices include fieldbus, Ethernet, Wi-Fi, Bluetooth LTE, cellular, LoRaWAN, and Sigfox, to name a few, since security approaches and requirements are different for each solution. On top of it all, many legacy industrial systems remain reliant upon outdated or proprietary protocols. This situation persists despite the awareness of vulnerabilities inherent within such protocols, typically due to a lack of any form of identification or authentication requirements.

IIoT device volume expands the cyberthreat landscape

Whether it's through the adoption of IoT devices and sensors retrofitted to legacy components, or through the connection of previously isolated internal systems to the external internet, the number of IIoT devices is growing dramatically, rising to 129.1 million devices in 2023, up from 85 million in 2020. This makes cybersecurity an even greater concern, due to the substantive increase in potential points of compromise.

This is not to say that every system is vulnerable to exploitation. Often, defensive countermeasures are implemented on top of legacy industrial deployments, including next-generation firewalls, intrusion detection or prevention systems, advanced threat protection systems, and other similar mechanisms. However, if these systems are going to remain reliant upon potentially vulnerable communication protocols, and they routinely become more connected to external networks, it is imperative that additional and redundant security measures be in place.

Recommendations for securing IIoT devices

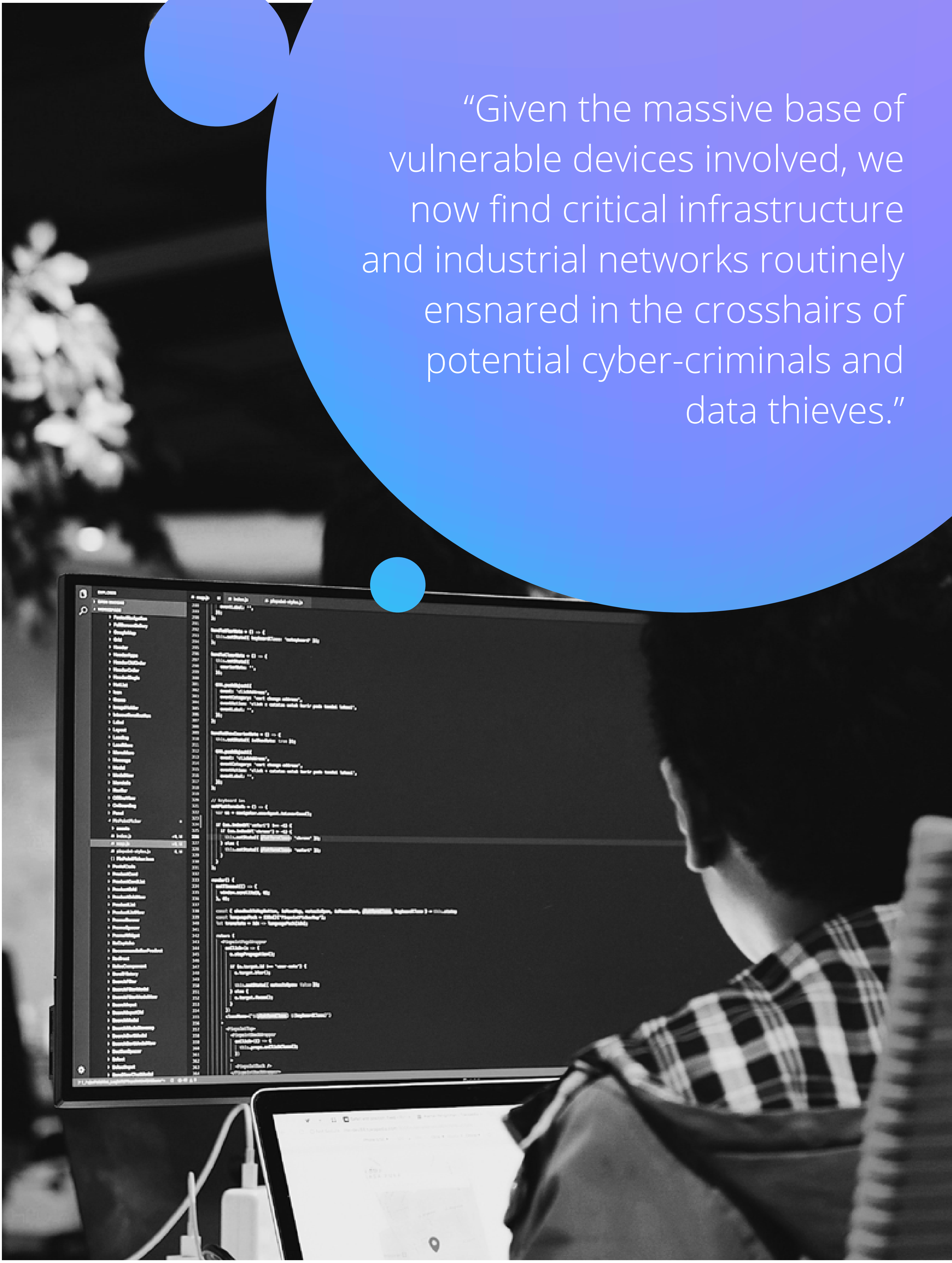
Any comprehensive approach to securing IoT devices in industrial settings will require the application of a multi-layered security platform. Defense in depth is a staple of every effective cybersecurity practice, and it calls for the implementation of several redundant measures of protection to ensure there is no single point of failure within the security ecosystem. The enforcement of such a strategy will help to mitigate the risks associated with the continued dependence and use of legacy systems.

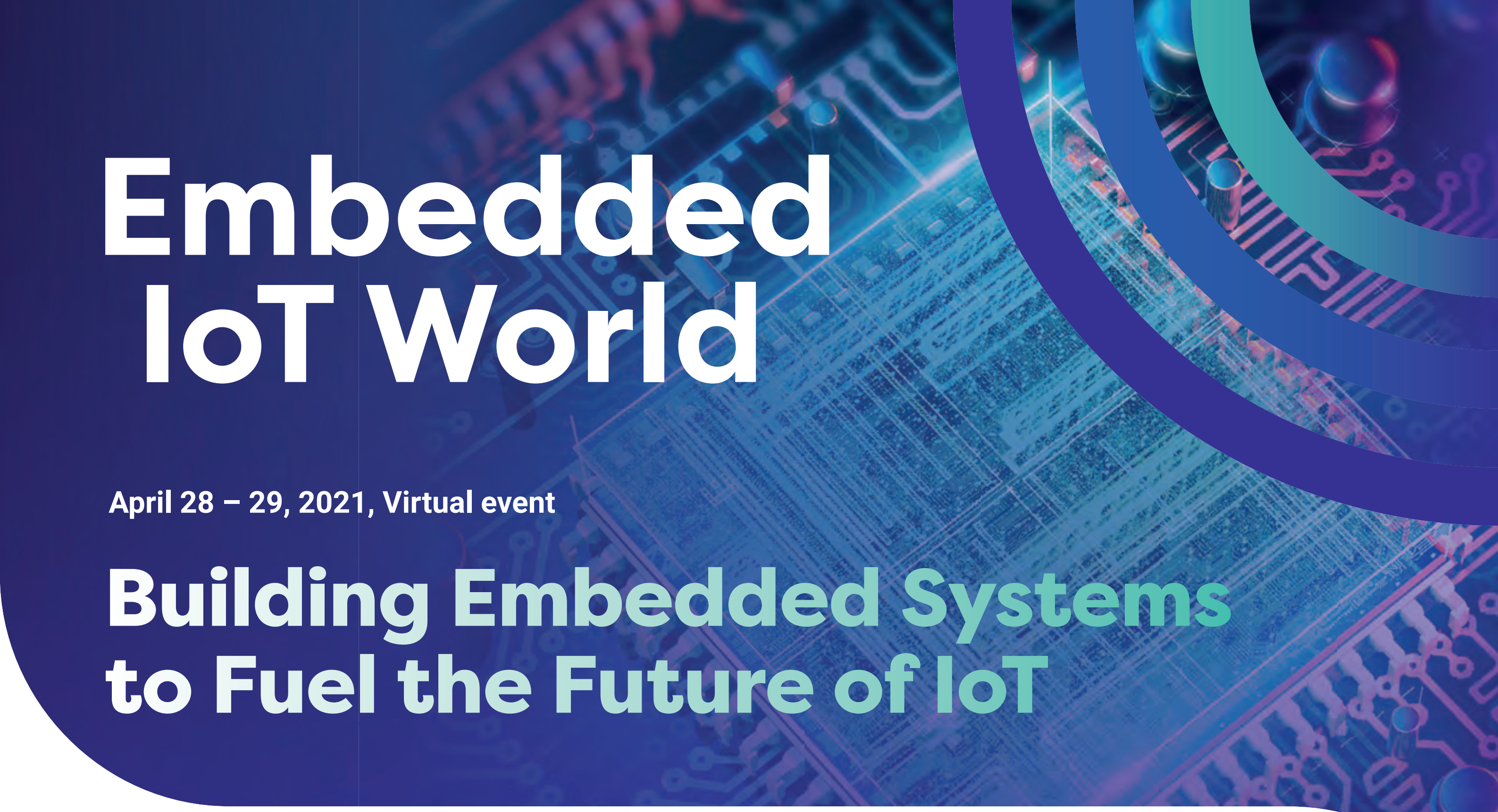
To be sure, vendors are already developing the next generation of embedded technologies for use in IoT devices, with a view to reinforcing industrial security; one example of how this is being carried out is through the utilization of cryptographic chipset architectures. Additionally, newer components and devices, including web gateways and advanced routers, are being designed with multiple security checks in place from the start, utilizing advanced identification, authentication, and authorization measures.

In the absence of mature standards specifically designed for IIoT, best practices exist within the enterprise and service provider domains. However, guidance will have to come from industrial leaders and IT teams that are deeply familiar with on-the-ground requirements and cost constraints. Organizations like the Industrial Internet Consortium, comprising tech industry leaders such as AT&T, Cisco, GE, IBM, and Intel, are working to provide an architectural framework for the IIoT. These efforts can help to provide a cohesive structure on which to build future industrial and critical infrastructure operations.

Yet one thing is certain: When it comes to securing IIoT networks, devices and data, substantive challenges will remain for many years to come.

“Given the massive base of vulnerable devices involved, we now find critical infrastructure and industrial networks routinely ensnared in the crosshairs of potential cyber-criminals and data thieves.”





Embedded IoT World

April 28 – 29, 2021, Virtual event

Building Embedded Systems to Fuel the Future of IoT

Unlock sponsorship opportunities

Amplify your brand influence and connect with technical professionals from around the world looking to partner and collaborate on end-to-end IoT solutions.

Industries

- Semiconductor Manufacturers
- Microcontroller/ Microprocessors
- Embedded Software
- Cellular & Connectivity
- Sensor Manufactures
- Chipset Manufacturers
- System Integrators
- Edge Computing & Processing
- Analytics
- Security
- RISC-V
- Platform & Enablement Companies

Job Titles

- Engineers
- Developers
- Architects
- Technologists
- Technicians
- Researchers
- Analysts
- CTOs
- Integrators
- Aggregators

Key topics on the agenda

- Device Security & Safety
- Processors & Instruction-Set Architecture
- Embedded Industrial IoT
- Edge Computing & Processing
- Connectivity
- AI & Machine Learning

Click here to find out more

Connecting the dots

Omdia is a global technology research powerhouse, established following the merger of the research division of Informa Tech (Ovum, Heavy Reading and Tractica) and the acquired IHS Markit technology research portfolio.*

We combine the expertise of over 400 analysts across the entire technology spectrum, analyzing 150 markets publishing 3,000 research solutions, reaching over 14,000 subscribers, and covering thousands of technology, media and telecommunications companies.

Our exhaustive intelligence and deep technology expertise allow us to uncover actionable insights that help our customers connect the dots in today’s constantly evolving technology environment and empower them to improve their businesses – today and tomorrow.

*The majority of IHS Markit technology research products and solutions were acquired by Informa in August 2019 and are now part of Omdia.

Contact us

Customer success

For dedicated customer assistance, connect with us now at **customersuccess@omdia.com**

Solutions & Product Information

For product inquiries or to speak to us, complete the form on our **website here.**

Non-Press Citations

For any research and data citation requests, connect with us now at **citations@omdia.com**

Press Inquiries

For any journalist inquiries and interviews, connect with us now at **press@omdia.com**

COPYRIGHT NOTICE AND DISCLAIMER

Disclaimer. The Omdia research, data and information referenced herein (the **“Omdia Materials”**) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact. The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result. Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials. To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

Internet of Things World

informa tech

All data correct as of 30.01.2020