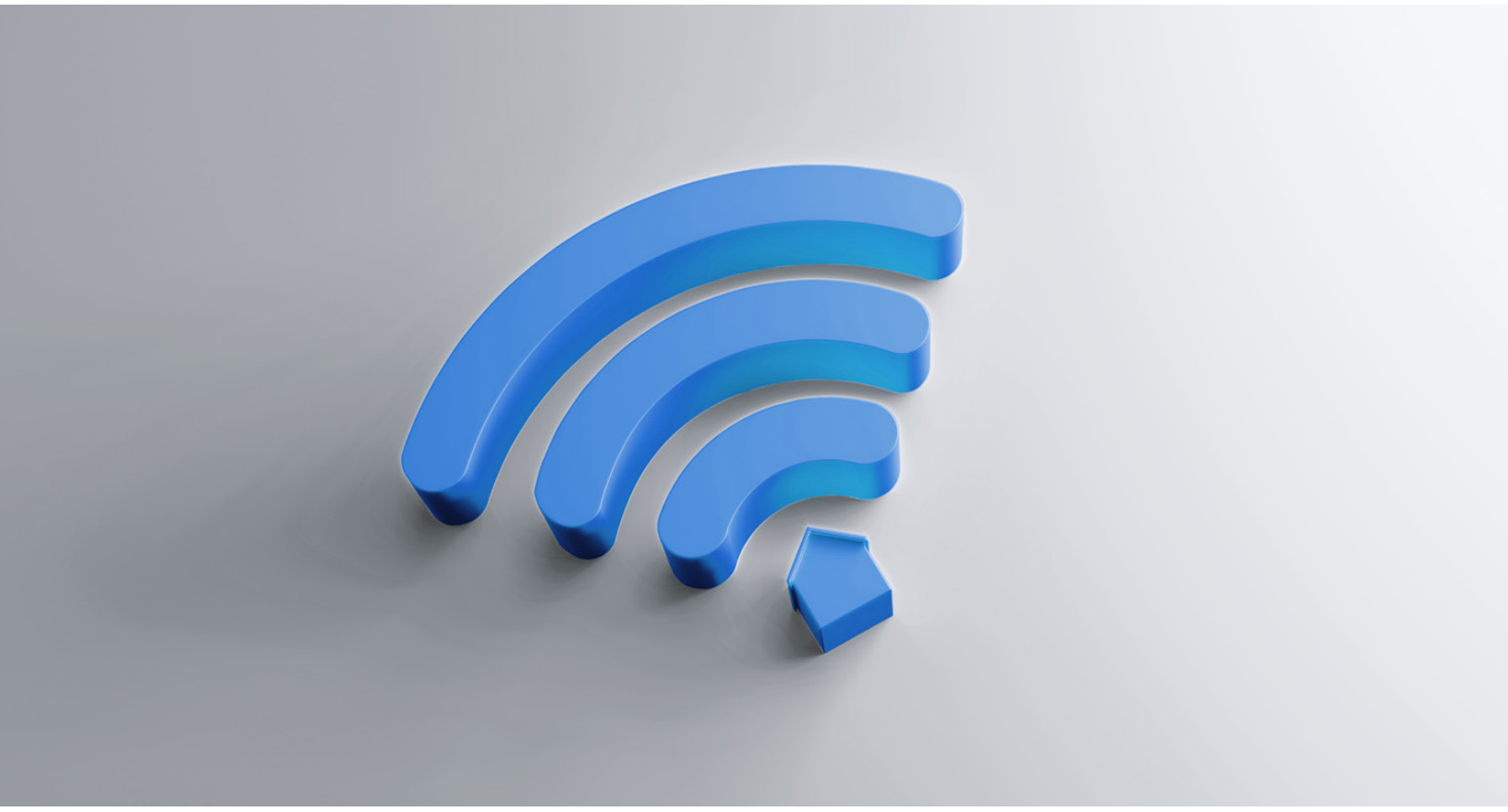
McKinsey & Company

McKinsey Explainers

What is the Internet of Things?

The Internet of Things (IoT) describes physical objects embedded with sensors and actuators that communicate with computing systems via wired or wireless networks—allowing the physical world to be digitally monitored or even controlled.



August 2022

Does your house have a smart thermostat? Or do you wear a fitness tracker to help you stay physically active? If you do, you are part of the Internet of Things, or IoT. It's become embedded in our lives, as well as in the way organizations operate.

IoT uses a variety of technologies to connect the digital and physical worlds. Physical objects are embedded with sensors—which can monitor things like temperature or motion, or really any change in environment—and actuators—which receive signals from sensors and then do something in response to those changes. The sensors and actuators communicate via wired (for example, Ethernet) or wireless (for example, WiFi, cellular) networks with computing systems that can monitor or manage the health and actions of connected objects and machines.

The physical objects being monitored don't have to be manufactured—they can include objects in nature, as well as people and animals. While some organizations might view IoT more expansively, our definition excludes systems in which all the embedded sensors are used just to receive intentional human input, such as smartphone apps, which receive data input primarily through a touchscreen, or other networked computer software, in which the sensors consist of a standard keyboard and mouse.

The constant connectivity that IoT enables, combined with data and analytics, provides new opportunities for companies to innovate products and services, as well as to increase the efficiency of operations. Indeed, IoT has emerged as one of the most significant trends in the digital transformation of business and the economy since the 2010s.

What are some IoT applications?

Looking at IoT applications, which are sometimes described as use cases, can help ground the discussion about what IoT is. Broadly, IoT applications occur in one of nine settings.

Human health. Devices can be attached to or inserted inside the human body, including wearable or ingestible devices that monitor or maintain health and wellness, assist in managing diseases such as diabetes, and more.

Home. Homeowners can install devices such as home voice assistants, automated vacuums, or security systems.

Retail environments. Devices can be installed in stores, banks, restaurants, and arenas to facilitate self-checkout, extend in-store offers, or help optimize inventory.

Offices. IoT applications in offices could entail energy management or security for buildings.

Standardized production environments. In such settings, including manufacturing plants, hospitals, or farms, IoT applications often aim to gain operating efficiencies or optimize equipment use and inventory.

Custom production environments. In customized settings like those in mining, construction, or oil and gas exploration and production, IoT applications might be used in predictive maintenance or health and safety efforts.

Vehicles. IoT can help with condition-based maintenance, usage-based design, or presales analytics for cars and trucks, ships, airplanes, and trains.

Cities. IoT applications can be used for adaptive traffic control, smart meters, environmental monitoring, or managing resources.

Outside. In urban environments or other outdoor settings, such as railroad tracks, autonomous vehicles, or flight navigation, IoT applications could involve real-time routing, connected navigation, or shipment tracking.

Other real-world examples abound. IoT solutions are being used in myriad settings: in refrigerators, to help restaurants optimize their food-compliance processes; in fields, to track livestock; in offices, to

track how many and how often meeting rooms are used; and beyond.

What is the economic impact of IoT?

The potential value of IoT is large and growing. By 2030, we estimate it could amount to up to $12.5 trillion globally. That includes the value captured by consumers and customers of IoT products and services.

The potential economic value of IoT differs based on settings and usages, with factory settings and human health applications representing outsize shares of this total. Factory settings could generate $1.4 trillion to $3.3 trillion by 2030, or just over a quarter of the total value potential. IoT economic impact in human health settings could reach around 14 percent of the total estimated value.

Another way of looking at IoT's value is to explore use-case clusters (similar uses adapted to different settings). Some of the most common use cases account for a sizable share of IoT's potential economic value:

— operations optimization, which is basically making the various day-to-day management of assets and people more efficient (41 percent)

— health (15 percent)

— human productivity (15 percent)

— condition-based maintenance (12 percent)

Other clusters include sales enablement, energy management, autonomous vehicles (the fastest-growing cluster), and safety and security.

What are IoT platforms?

To get value from IoT, it helps to have a platform to create and manage applications, to run analytics, and to store and secure your data. Essentially, these platforms do a lot of things in the background to make life easier and less expensive for developers, managers, and users—in much the same way as an operating system for a laptop. They handle issues like connecting and extracting data from many different endpoints, which might be in inconvenient locations with spotty connectivity.

If you are trying to choose an IoT platform, you'll need a good understanding of your company's IoT strategy. Here are five characteristics to consider when evaluating IoT platforms:

1. *Applications environment*. Here, you might examine questions like: Can the platform develop, test, and maintain multiple applications? Can it connect easily to the applications your company already uses, for example, for enterprise resource planning?

2. *Data management.* When weighing this element, it's helpful to understand if the platform can structure and join multiple unfamiliar data sets, for example.

3. *Ownership of cloud infrastructure.* Does the infrastructure provider own and operate its own data centers, or which public cloud provider does it use? (See "What is cloud computing?" for even more on this topic.)

4. *Security.* What commercial-grade authentication, encryption, and monitoring capability does the platform have, and are they distinctive?

5. *Edge processing and control.* Here, you could examine whether the platform can do edge analytics, without first bringing data into the cloud, or whether it can be easily configured to control local assets without human intervention.

What should I know about IoT security?

The billions of IoT devices in use have naturally created new vulnerabilities for companies. As more "things" get connected, the number of ways to attack them mushrooms. Pre-IoT, a large corporate network might have needed to account for 50,000

to 500,000 endpoints being vulnerable to attack, while the IoT may involve a network with millions or tens of millions of these endpoints. Promoting cybersecurity, therefore, is crucial in the IoT era.

It's important to address customer privacy concerns vis-à-vis connected devices. But managing IoT cybersecurity is also about protecting critical equipment, such as pacemakers or entire manufacturing plants—which, if attacked, could put your customers' health or your company's total production capability at risk.

Six recommendations or actions could help CEOs and other leaders tackling IoT cybersecurity:

— understand what IoT security will mean for your industry and business model

— set clear roles and responsibilities for IoT security in your supply chain

— hold strategic conversations with regulators and collaborate with other industry players

— view cybersecurity as a priority for the entire product life cycle, and develop skills to achieve it

— transform mindsets and skills rigorously

— create a point-of-contact system for external security researchers and implement a postbreach response plan

What is IIoT?

The Industrial Internet of Things, or IIoT, is among the advanced manufacturing technologies collectively referred to as Industry 4.0, or the Fourth Industrial Revolution.

What are some benefits of IIoT? It can drastically reduce downtime, open up new business models, and improve customer experience—and it can also make organizations more resilient. In the COVID-19 era, for example, digital management tools and constant connectivity allowed some companies to react to market changes swiftly and efficiently by quickly adjusting production capacity and simultaneously supporting remote operations.

Companies using IIoT for digital transformation in manufacturing can follow seven guideposts to align their business, organization, and technology spheres and help leaders successfully position their organizations to reap the full benefits from IIoT:

— Business

- identify and prioritize use cases
- focus on plant rollout and enablement

— Organization

- keep an eye on change and performance management
- build capabilities and embrace new ways of working

— Technology

- attend to IIoT and data infrastructure, with a focus on core platform design, including IT/OT (information technology/operational technology) cybersecurity
- choose an IIoT platform given the cloud imperative in manufacturing
- watch the tech ecosystem

What do I need to know about Internet of Things B2B uses?

Internet of Things B2B solutions account for the majority of economic value created from IoT to date. In B2B settings, for example, marrying IoT

and AI can improve the predictive-maintenance capabilities of machines, while also empowering service providers to watch the health of their assets in real time, proactively addressing issues before a bigger breakdown occurs.

B2C applications have grown faster than expected, particularly given the adoption of home-automation solutions. However, through 2030, B2B applications are projected to nonetheless account for 62 to 65 percent of total IoT value.

What dynamics could affect IoT adoption?

When it comes to getting more value from IoT, there are tailwinds as well as headwinds that will affect IoT adoption.

Three factors could accelerate the adoption of and impact from IoT solutions:

— *The perceived value proposition.* Customers see value in IoT, and the way it enables digital transformation and sustainability efforts—as evidenced by the $1.6 trillion in economic value generated from IoT solutions in 2020.

— *Technology*. Affordable technology, which enables IoT deployments at scale, exists for the vast majority of IoT applications. And progress in hardware can be coupled with developments in analytics, AI, and machine learning, which can enable more granular insights and faster decision making.

— *Networks.* These are the backbone of IoT, and higher-performing 4G and 5G networks are now available to more people.

Conversely, a variety of factors could constrain adoption. These include the need for change management (capturing value at scale will require collaboration across functions to encourage new behaviors), interoperability issues, and installation challenges, as well as concerns about cybersecurity and individual privacy.

If your organization is just getting started, it can be helpful to consider what could accelerate enterprise IoT journeys. An interview with Wienke Giezeman, a serial tech entrepreneur and initiator of The Things Network, offers insight on what can drive action: “We’ve seen this in the industry again and again—you cannot solve IoT problems with money. It’s so tempting to try to solve these problems with cash, but really, it’s the creativity and pushing for simplicity that leads to the solution, which shouldn’t be so complicated.”

Is there value in scaling IoT efforts?

To really see the benefits of IoT, companies must embrace the technology at scale, instead of making one-off efforts. If your organization is adopting IoT, here are seven useful actions for scaling IoT:

— decide who owns IoT in the organization

— design for scale from the start

— don’t dip your toe in the water—deploying multiple use cases can be a forcing mechanism in transforming operating models, workflows, and processes

— invest in technical talent

— change the entire organization, not just the IT function

— push for interoperability

— proactively shape your environment by building and controlling IoT ecosystems

Articles referenced include:

— “IoT comes of age,” March 7, 2022, Michael Chui and Mark Collins

— “IoT value set to accelerate through 2030: Where and how to capture it,” November 9, 2021, Michael Chui, Mark Collins, and Mark Patel

— “A manufacturer’s guide to scaling Industrial IoT,” February 5, 2021, Andreas Behrendt, Enno de Boer, Tarek Kasah, Bodo Koerber, Niko Mohr, and Gérard Richter

— “Industry 4.0 adoption with the right focus,” October21, 2021, Matteo Mancini, Gustavo Marteletti, Alpesh Patel, Laura Requeno, and Tingfeng Ye

— “From defense to offense: Digital B2B services in the next normal,” August 28, 2020, Guy Benjamin, Markus Forsgren, and Nicolas Guzman

Designed by McKinsey Global Publishing