[Internet of things (IoT)](https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT)

[IoT devices (internet of things devices)](https://www.techtarget.com/iotagenda/definition/IoT-device)

The internet of things, or IoT, is a network of interrelated devices that connect and exchange data with other [IoT devices](https://www.techtarget.com/iotagenda/definition/IoT-device) and the cloud. IoT devices are typically embedded with technology such as sensors and software and can include mechanical and digital machines and consumer objects.

How does IoT work?

An IoT ecosystem consists of web-enabled smart devices that use embedded systems -- such as processors, sensors, and communication hardware -- to collect, send and act on data they acquire from their environments.

IoT devices share the [sensor data](https://www.techtarget.com/iotagenda/definition/sensor-data) they collect by connecting to an [IoT gateway](https://www.techtarget.com/iotagenda/definition/IoT-gateway), which acts as a central hub where IoT devices can send data. Before the data is shared, it can also be sent to an [edge device](https://www.techtarget.com/searchnetworking/definition/edge-device) where that data is analyzed locally. Analyzing data locally reduces the volume of data sent to the cloud, which minimizes bandwidth consumption.

Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for example, to set them up, give them instructions or access the data.



### Why is IoT important?

IoT helps people live and work smarter. Consumers, for example, can use IoT-embedded devices -- such as cars, smartwatches or thermostats -- to improve their lives. For example, when a person arrives home, their car could communicate with the garage to open the door; their thermostat could adjust to a preset temperature; and their lighting could be set to a lower intensity and color.

In addition to offering smart devices to automate homes, IoT is essential to business. It provides organizations with a real-time look into how their systems really work, delivering insights into everything from the performance of machines to [supply chain](https://www.techtarget.com/whatis/definition/supply-chain) and logistics operations.

IoT enables machines to complete tedious tasks without human intervention. Companies can automate processes, reduce labor costs, cut down on waste and improve service delivery. IoT helps make it less expensive to manufacture and deliver goods, and offers transparency into customer transactions.

IoT is one of the most important technologies and it continues to advance as more businesses realize the potential of connected devices to keep them competitive.

### What are the benefits of IoT to organizations?

[IoT offers several benefits to organizations](https://www.techtarget.com/iotagenda/tip/Top-advantages-and-disadvantages-of-IoT-in-business). Some benefits are industry-specific and some are applicable across multiple industries. Common benefits for businesses include the following:

* Monitors overall business processes.
* Improves the customer experience.
* Saves time and money.
* Enhances employee productivity.
* Provides integration and adaptable business models.
* Enables better business decisions.
* Generates more revenue.

IoT encourages companies to rethink how they approach their businesses and gives them the tools to improve their business strategies.

Generally, IoT is most abundant in manufacturing, transportation and utility organizations that use sensors and other IoT devices; however, it also has use cases for organizations within the agriculture, infrastructure and home automation industries, leading some organizations toward [digital transformation](https://www.techtarget.com/searchcio/definition/digital-transformation).

IoT can benefit farmers in agriculture by making their job easier. Sensors can collect data on rainfall, humidity, temperature and soil content and IoT can help automate farming techniques.

IoT can also help monitor operations surrounding infrastructure. Sensors, for example, can monitor events or changes within structural buildings, bridges and other infrastructure that could potentially compromise safety. This provides benefits such as improved incident management and response, reduced costs of operations and improved quality of service.

A home automation business can use IoT to monitor and manipulate mechanical and electrical systems in a building. On a broader scale, smart cities can help citizens reduce waste and energy consumption.

IoT Device

Internet of things ([IoT](https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT)) devices are nonstandard computing hardware -- such as sensors, actuators or appliances -- that connect wirelessly to a network and can transmit data.

IoT extends internet connectivity beyond typical computing devices -- such as desktops, laptops, smartphones and tablets -- to any range of traditionally *dumb* or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the internet, and can be remotely monitored and controlled.

IoT devices have both industrial and consumer uses and are typically integrated into other tools such as mobile devices, industrial equipment and medical devices. Over a broad range, they can also be [used in smart cities](https://www.computerweekly.com/news/366543653/Berlin-ranked-top-smart-city-in-Europe-in-2023). They're then used to send data or interact with other IoT devices over a network.

IoT and IoT devices aid in making daily activities faster, easier or more convenient for consumers while also providing real-time data for industrial or enterprise use cases.

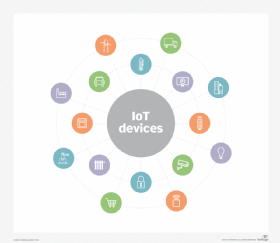
### What is an example of an IoT device?

Connected devices are part of an ecosystem in which every device talks to other related devices in the environment to automate home and industry tasks. They can transmit [sensor data](https://www.techtarget.com/iotagenda/definition/sensor-data) to users, businesses and other intended parties. The devices can be categorized into three main groups: consumer, enterprise and industrial.

**Consumer-connected devices** include smart TVs, smart speakers such as Google Home, toys, [wearables](https://www.techtarget.com/searchmobilecomputing/definition/wearable-technology) and smart appliances. In a [smart home](https://www.techtarget.com/iotagenda/definition/smart-home-or-building), for example, IoT devices are designed to sense and respond to a person's presence. When a person arrives home, their car communicates with the garage to open the door. Once inside, the thermostat is already adjusted to a preset temperature, and the lighting is set to a lower intensity and color. Other smart home devices include sprinklers that adjust the amount of water distributed on the lawn based on the weather forecast and robotic vacuum cleaners that learn which areas of the home must be cleaned most often.

**Enterprise IoT devices** are [edge devices](https://www.techtarget.com/searchnetworking/definition/edge-device) designed for businesses. There are a wide variety of enterprise IoT devices available. These devices vary in capabilities but tend to be geared toward maintaining a facility or improving operational efficiency. Some options include smart locks, smart thermostats, smart lighting and smart security. Consumer versions of these technologies exist as well.

In the enterprise, smart devices can help with meetings. [Smart sensors](https://www.techtarget.com/iotagenda/definition/smart-sensor)located in a conference room can help an employee locate and schedule an available room for a meeting, ensuring the proper room type, size and features are available.

Consumer, enterprise and industrial IoT devices include smart TVs and smart sensors outfitted for conference rooms and assembly line machines.

Likewise, retailers can [use RFID tags](https://www.techtarget.com/searcherp/tip/RFID-vs-IoT-What-are-the-differences) to track a business's goods, increasing inventory accuracy. Expanding on this idea, IoT devices are also used to keep track of inventory as it moves along in the supply chain for [supply chain management](https://www.techtarget.com/searcherp/definition/supply-chain-management-SCM).

**Industrial IoT (IIoT) devices** are designed for use in factories or other industrial environments. Most [IIoT](https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT) devices are sensors used to monitor an assembly line or other manufacturing processes. Sensor data is transmitted to monitor applications to ensure key processes are running optimally. These same sensors can also prevent unexpected downtime by predicting when parts need to be replaced.

If a problem occurs, the system can send a notification to a service technician informing them of what's wrong and what parts they need to fix the problem. This can save the technician from coming on site to diagnose the problem and then having to travel to a warehouse to get the part needed to fix the problem.

In the medical industry, IoT devices are used to monitor a patient's health and track their vitals. If a patient needs attention, these monitors send notifications to the relevant healthcare workers.

### How do IoT devices work?

IoT devices vary in terms of functionality, but also have some similarities in how they work. First, IoT devices are physical objects designed to interact with the real world in some way. The device might be a sensor on an assembly line or an intelligent security camera. In either case, the device senses what's happening in its surrounding environment.

The devices themselves typically include an integrated CPU, firmware and a network adapter. In most cases, IoT devices connect to a [Dynamic Host Configuration Protocol](https://www.techtarget.com/searchnetworking/definition/DHCP) server and acquire an IP address that it can use to function on the network. Some IoT devices are directly accessible over the public internet, but most are designed to operate exclusively on private networks.

Although not an absolute requirement, many IoT devices are configured and managed through a software application. Some devices, however, have integrated web servers, eliminating the need for an external application.

Once an IoT device has been configured and begins to operate, most of its traffic is outbound. A security camera, for example, streams video data. Likewise, an industrial sensor streams sensor data. Some IoT devices such as smart lights, however, do accept inputs.

### What is IoT device management?

Several challenges can hinder the successful deployment of an IoT system and its connected devices, including security, interoperability, power and processing capabilities, scalability and availability. Many of these problems can be addressed with [IoT device management](https://www.techtarget.com/iotagenda/definition/internet-of-things-device-management-IoT-device-management), either by adopting standard protocols or using services offered by a vendor.

Device management helps companies integrate, organize, monitor and remotely manage internet-enabled devices at scale, offering features critical to maintaining the health, connectivity and security of the IoT devices along their entire lifecycles.

IoT device management contains separate categories, including onboarding devices, configuration, maintenance, diagnostics and end-of-life management. Device management typically follows a pattern such as the following:

* Registration and activation.
* Authentication and authorization.
* Configuration.
* Provisioning.
* Monitoring and diagnostics.
* Troubleshooting.
* Firmware updates.

Some examples of standardized device management protocols include the Open Mobile Alliance device management and Lightweight Machine to Machine.

IoT device management services and software are also available from vendors, including Amazon, General Electric, Google, IBM and Microsoft.

### IoT device connectivity and networking

The networking, communication and connectivity protocols used with internet-enabled devices largely depend on the specific IoT application deployed. Just as there are many different IoT applications, there are many different connectivity and communication options, including the following:

* Constrained Application Protocol, or CoAP.
* Datagram Transport Layer Security, or DTLS.
* [MQ Telemetry Transport](https://www.techtarget.com/iotagenda/definition/MQTT-MQ-Telemetry-Transport), or MQTT.
* Data Distribution Service, or DDS.
* Advanced Message Queuing Protocol, or AMQP.

Wireless protocols include the following:

* [IPv6](https://www.techtarget.com/searchnetworking/definition/IPv6-Internet-Protocol-Version-6).
* Zigbee [Bluetooth Low Energy](https://www.techtarget.com/iotagenda/definition/Bluetooth-Low-Energy-Bluetooth-LE).
* [Z-Wave](https://www.techtarget.com/iotagenda/definition/Z-Wave).

Cellular, satellite, Wi-Fi and Ethernet can also be used.

Connectivity options have tradeoffs in terms of power consumption, range and bandwidth, all of which must be considered when choosing connected devices and protocols for an IoT application. These options range from high range, power consumption and bandwidth to low range, power consumption and bandwidth to high range, but low power consumption and bandwidth.

In most cases, IoT devices connect to an [IoT gateway](https://www.techtarget.com/iotagenda/definition/IoT-gateway)or another edge device where data can either be analyzed locally or sent to the cloud for analysis. Some devices have integrated data processing capabilities that minimize the amount of data that must be sent to the cloud or to the data center. This type of processing, which often uses machine learning capabilities that are integrated into the device, is becoming increasingly popular as IoT devices create more data.

### What security risks do IoT devices pose?

The interconnection of traditionally dumb devices raises several questions in relation to security and privacy. As is often the case, IoT technology has moved more quickly than the mechanisms available to safeguard devices and their users.

Some of the top IoT security risks that organizations should address include the following:

* Increased attack surfaces.
* Unsecured hardware.
* Poor asset management.
* [Shadow IoT](https://www.techtarget.com/searchcloudcomputing/definition/shadow-IT-shadow-information-technology).
* Unencrypted data transmissions.
* Domain name system ([DNS](https://www.techtarget.com/searchnetworking/definition/domain-name-system)) threats.
* Malicious node injections.
* IoT ransomware attacks.
* Firmware exploits.

One of the largest demonstrated remote hacks on IoT-connected devices occurred in October 2016. A distributed [denial-of-service](https://www.techtarget.com/searchsecurity/definition/denial-of-service) attack dubbed the Mirai botnet affected DNS on the east coast of the U.S, disrupting services worldwide -- an issue traced back to hackers infiltrating networks through IoT devices, including wireless routers and connected cameras. Similarly, in 2020, an IoT data breach occurred when a cybersecurity expert took advantage of a massive Bluetooth vulnerability and hacked a Tesla Model X in less than 90 seconds without so much as triggering an alarm.

Safeguarding IoT devices and the networks they connect to can be challenging due to the variety of devices and vendors, as well as the difficulty of adding security to resource-constrained devices. In the case of the Mirai botnet, the problem was traced back to the use of default passwords on the hacked devices.

Suggested IoT security measures include the following:

* [Authentication](https://www.techtarget.com/searchsecurity/definition/authentication) and authorization and identity management.
* Cryptography.
* Encryption.
* Network segmentation.
* Strong passwords.

Concerned by the dangers posed by the rapidly growing [IoT attack surface](https://www.techtarget.com/iotagenda/definition/IoT-attack-surface), the FBI released the public service announcement FBI Alert Number I-091015-PSA in September 2015, which is a document outlining the risks of IoT devices, as well as protections and defense recommendations.

In December 2020, the IoT Cybersecurity Improvement Act of 2020 was signed into law by former President Donald Trump. This law directed the National Institute of Standards and Technology ([NIST](https://www.techtarget.com/searchsoftwarequality/definition/NIST)) to develop and publish standards and guidelines on the use and management of IoT devices. Although these standards were originally intended for use by federal agencies, NIST developed in 2022 a pilot program for IoT security device labeling for consumers. Using NIST's criteria, in 2023, the Biden administration launched the U.S Cyber Trust Mark, which aims to provide U.S. consumers with labelled products that meet these established security criteria.